Tunis Re

...à la hauteur de vos risques

Les Risques Émergents

Les Risques Émergents

Dossier élaboré par :

Mme Henda SEBAI

Mme Asma NAIMI

M. Aymen BOULARES

Sommaire

Introduction

Les assureurs et les réassureurs sont aujourd'hui confrontés à un degré de changement et d'incertitude qui semble évoluer à un rythme toujours plus rapide et la gestion des risques a toujours été au cœur de l'activité des organismes d'assurance. Elle est une fonction clé de leur système de gouvernance. Toutefois, cette notion de risque se complexifie aujourd'hui et se focalise naturellement sur les risques émergents.

Les risques émergents sont définis par des risques nouveaux ou changeants qui sont difficiles à quantifier et qui pourraient avoir un impact majeur sur la société et l'industrie. De plus, ce sont des risques dont le danger potentiel n'est pas encore connu de manière fiable et dont les implications sont difficiles d'accès. De ce fait, il semblerait que les risques émergents soient, de par leur nature, non modélisables.

Dans ce contexte, les assureurs et réassureurs sont inévitablement amenés à considérer ces risques comme des opportunités pour leur entreprise, tant ces derniers peuvent en effet déboucher sur un élargissement de l'offre d'assurance, avec le développement de nouveaux produits ou de nouvelles garanties. Néanmoins, ils constituent aussi des menaces pour leur rentabilité.

Cette incertitude caractérisant les risques émergents provient d'un certain manque d'observations historiques que constituent par définition les risques nouveaux, mais aussi les mutations scientifiques, technologiques ou socio-politiques.

Les risques émergents identifiés par les experts comme ayant un impact sur le monde de l'assurance et de la réassurance sont classés en six groupes principaux : risque économique, environnemental, sociétal, technologique, politique et, dans une moindre mesure, réglementaire.

De plus, Les risques émergents doivent être étudiés de manière plus analytique afin de prendre des mesures pratiques pour y faire face et créer de la valeur pour le secteur de l'assurance. Ils sont classés en trois catégories par les experts : technologiques, cristallisants et aggravants :

Les risques technologiques sont ceux qui sont réellement nouveaux, qui émergent des nouvelles technologies et procédés. Cette catégorie comprendrait les risques associés à la cyber-technologie, les organismes génétiquement modifiés, la nanotechnologie, les cigarettes électroniques, les voitures sans conducteur…

Les risques cristallisants sont ceux qui ne sont pas nouveaux, mais dont la manifestation et les implications émergent. Dans ce contexte nous regardons autant les pertes émergentes que les risques émergents. Cette catégorie comprendrait les risques de l'amiante et de l'aluminium sur la santé.

Les risques aggravants sont relativement bien connus, mais où leur incidence et leur impact sont devenus potentiellement plus aggravés. Cette catégorie comprendrait le changement climatique, les pandémies, la résistance aux antibiotiques, le terrorisme…

Ces catégories ne sont pas des compartiments étanches, certains risques émergents contiennent des éléments des trois catégories. Cependant, une focalisation sur la caractéristique prédominante permet de voir que chaque catégorie nécessite une action différente.

Quelle que soit la catégorie de risque émergent, le principal défi réside dans la modélisation et la quantification de leurs impacts potentiels. Ce n'est qu'ainsi que les assureurs et les réassureurs tirent parti de leur capacité clé, qui est la création de valeur par gestion des risques.

Risques Emergents

1. Faire face aux risques des changements climatiques : Nouveaux enjeux pour le secteur de l'Assurance et de la Réassurance

Introduction

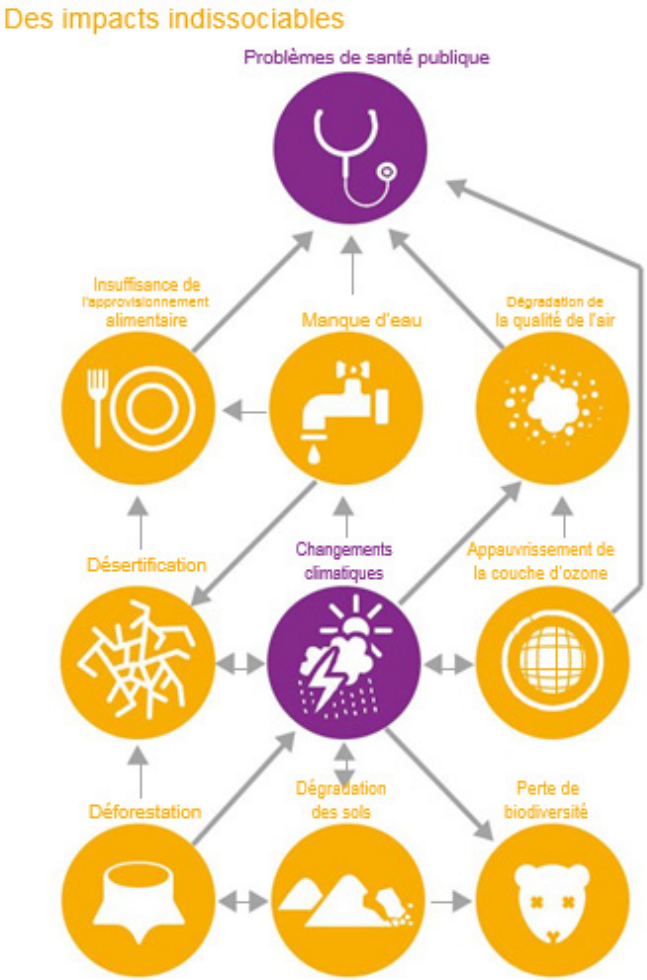
Les observations faites par rapport aux changements climatiques pendant plusieurs décennies, ainsi que les projections climatiques fournissent des preuves irréfutables sur la vulnérabilité des ressources en eau douce de la planète, celles-ci sont potentiellement exposées aux impacts des changements climatiques, avec des conséquences ayant des grandes ampleurs sur les Humains et les écosystèmes.

Le réchauffement observé sur plusieurs décennies est étroitement lié aux changements du cycle hydrologique à grande échelle tels que: l'augmentation de la teneur en vapeur d'eau atmosphérique; le changement des régimes de précipitation, l'occurrence d'évènements hydrologiques extrêmes, la fonte de glace; et les conséquences de ces évènements sur le ruissellement, aussi bien que la qualité des sols qui voient leur humidité varier. Les changements de précipitations, considéré comme principal impact du CC sur les ressources en eau, montre une variabilité spatiale et inter-décennale.

L'augmentation de l'intensité et de la variabilité des précipitations devrait augmenter les risques de crue et de sécheresse dans plusieurs régions. En effet, la fréquence des épisodes de fortes précipitations augmentera ayant pour conséquence directe un accroissement des risques de crues d'origine pluviale. En même temps, le pourcentage de la superficie terrestre soumis à une sécheresse extrême à un moment donné devrait augmenter.

L'augmentation de la température des eaux et les variations des phénomènes extrêmes, notamment les crues et les sécheresses, devraient influencer la qualité de l'eau et aggraver de nombreuses formes de pollution aquatique : ayant des conséquences sur la sédimentation, les nutriments, le carbone organique dissous, etc les éventuelles conséquences néfastes sur les équilibres des écosystèmes sont nombreuses.

Impacts des changements climatiques



Impacts sur l'agriculture et sécurité alimentaire, utilisation des terres et foresterie

La productivité des systèmes agricoles et forestiers et des pêcheries dépend en grande partie de la distribution temporelle et spatiale des précipitations et de l'évaporation, ainsi que de la disponibilité des ressources en eau douce pour l'irrigation, en particulier pour les cultures. Avec le changement climatique, les systèmes de production sont devenus de plus en plus sensibles, particulièrement dans les régions qui sont d'ores et déjà vulnérables, ils sont confrontés à un accroissement des risques liés à l'instabilité climatique, en l'occurrence concernant l'eau suite à plusieurs facteurs conséquents, dont la dégradation des terres et sols par l'érosion, la surexploitation des eaux souterraines et la salinisation correspondante des aquifères et des sols.

Dans ce contexte, les petites exploitations sont particulièrement vulnérables au changement climatique et la variabilité du climat, d'autres facteurs de stress socioéconomique viennent souvent aggraver des conditions environnementales déjà difficiles.

Dans les forêts par exemple, on a démontré que les incendies et les pullulations d'insectes liés à la fréquence de phénomènes extrêmes augmentent la vulnérabilité au climat.

L'eau joue un rôle prépondérant dans la production alimentaire au niveau régional et mondial. D'un côté, plus de 80 % des terres agricoles mondiales ne sont pas irriguées. Pour ces régions, la productivité des cultures dépend uniquement de la pluie, l'évapotranspiration et l'humidité des sols. Lorsque ces variables sont limitées par le climat, comme dans les régions arides et semi-arides, la production agricole devient très vulnérable au changement climatique.

D'un autre côté, les ressources en eau disponibles pour l'irrigation agissent également sur la production mondiale d'aliments. En effet, les terres irriguées, qui ne représentent que 18 % des terres agricoles mondiales, produisent 1 milliard de tonnes de blé par an, à savoir environ la moitié de l'approvisionnement total du monde. Cela s'explique par le rendement des cultures irriguées qui est de 2 à 3 fois plus élevé en moyenne que celui des terres non irriguées.

Tandis qu'un déficit d'eau entraîne la vulnérabilité de la production, l'excès d'eau peut également avoir des effets préjudiciables sur la productivité des cultures, soit directement, par exemple en affectant les propriétés du sol et en perturbant la croissance des plantes, soit indirectement, par exemple en troublant ou en retardant les actions nécessaires pour l'exploitation. Des phénomènes de pluies intenses, une humidité excessive dans le sol et les inondations perturbent la production d'aliments et les moyens de subsistance ruraux au niveau mondial

Les contraintes socioéconomiques des prochaines décennies entraîneront une augmentation de la compétition entre les besoins pour l'irrigation et la demande des secteurs non agricoles, et réduiront potentiellement la disponibilité et la qualité des ressources en eau pour les aliments. Le changement climatique pourrait davantage réduire la disponibilité en eau pour la production alimentaire mondiale du fait des changements moyens prévus des régimes de température et de précipitations, mais également du fait de l'augmentation prévue de la fréquence des phénomènes extrêmes, tels que les sécheresses et les inondations.

Impacts sur la santé humaine

La santé humaine, qui englobe le bien-être physique, social et psychologique, dépend entre autres d'un approvisionnement adéquat en eau potable et d'un environnement sûr. Les êtres humains sont directement exposés au changement climatique via des configurations météorologiques (phénomènes extrêmes plus intenses et plus fréquents), et indirectement via des changements de l'eau, de l'air, de la qualité et de la quantité des aliments, des écosystèmes, de l'agriculture, des moyens de subsistance et des infrastructures.

En raison du très grand nombre de personnes risquant d'être touchées, la malnutrition et la rareté de l'eau pourraient être les conséquences les plus importantes du changement climatique sur la santé.

Quoique la santé des populations s'est remarquablement améliorée au fil des 50 dernières années, mais il persiste des inégalités substantielles d'un pays à l'autre et au sein même des pays. Les objectifs visant à réduire le taux de mortalité chez les enfants de moins de cinq ans paraissent difficilement réalisables dans certains pays en développement. La fragilité de ces populations augmente leur vulnérabilité et réduit leur capacité de s'adapter et de résilier face aux changements climatiques. Les populations aux taux élevés d'occurrence des maladies et de handicaps résistent moins bien aux stress de toutes sortes, y compris ceux liés au changement climatique.

Impacts sur les établissements humains et les infrastructures

Les changements de la disponibilité en eau, de la qualité de l'eau, et des caractéristiques des précipitations, ainsi que la probabilité et l'ampleur des épisodes d'inondations devraient jouer un rôle important dans les incidences du changement climatique sur les établissements humains et les infrastructures.

Ces incidences varieront d'une région à l'autre. De plus, les incidences dépendront en grande partie du cadre géophysique, du niveau de développement socioéconomique, de la nature de la base économique locale, des caractéristiques des infrastructures et d'autres facteurs sources de stress. Ces derniers englobent la pollution, la dégradation des écosystèmes, l'affaissement des terres et la croissance démographique.

Les inondations dues à l'élévation du niveau de la mer et à l'augmentation de l'intensité des phénomènes météorologiques extrêmes (tels les tempêtes et les ouragans) représentent un danger pour les réseaux de transport dans certaines régions.

Ces dangers sont l'inondation localisée des rues, des réseaux de transports souterrains et les dommages subis par les ponts, les routes et les voies ferrées liés aux crues et aux glissements de terrain.

Impacts sur l'économie : assurance, industrie, tourisme et transport

Le climat a une influence sur plusieurs secteurs secondaires et tertiaires de l'économie tels que les assurances, l'industrie, le tourisme et les transports. Les phénomènes climatiques extrêmes entrainant des changements brusques ont tendance à affecter les systèmes humains plus sévèrement que le changement progressif, en partie car ils laissent moins de temps pour l'adaptation.

Les pertes mondiales révèlent une augmentation rapide des coûts dépensés suite à des épisodes météorologiques extrêmes, et ce depuis les années 1970. Il existe aussi des preuves d'une augmentation de l'occurrence pour des régions et des dangers spécifiques, y compris les crues extrêmes notamment si elles touchent des grands fleuves et rivières.

Pour démontrer la grande incidence de la variabilité climatique sur les pertes des assurances, on peut citer par exemple que les inondations sont responsables de 10 % des pertes des assurances liées aux phénomènes météorologiques à l'échelle planétaire.

La sécheresse a également une incidence : les données du Royaume-Uni indiquent une relation décalée entre le coût des déclarations de sinistres liés à la subsidence et aux faibles précipitations.

Cependant, dans les pays en développement, les pertes résultant de phénomènes extrêmes sont mesurées plus en termes de vies humaines qu'en termes d'assurances. Par exemple, malgré sa grande intensité, la sécheresse du Sahel n'a eu qu'une faible incidence sur le secteur financier formel, en raison de la faible pénétration des assurances.

Coûts socioéconomiques, atténuation, adaptation, vulnérabilité et développement durable

De toutes les éventuelles incidences liées aux changements climatique sur les transports, le coût le plus élevé est imputable aux inondations. Les secteurs industriels sont souvent considérés comme

étant moins vulnérables aux incidences du changement climatique que des secteurs tels celui de l'agriculture.

Parmi les principales exceptions, on trouve les installations industrielles situées dans des régions sensibles au climat (telles que des plaines inondables) et celles dépendant de produits de base sensibles au climat, telles que les installations de transformation des aliments.

La couverture par les assurances actuellement disponible dans un pays pour les risques spécifiques devra être adaptée à l'incidence des catastrophes passées. En raison de la concentration élevée de pertes dues aux crues et catastrophes climatiques, l'assurance du secteur privé contre ces phénomènes est généralement restreinte (voire non existente), de telle sorte que dans plusieurs pays, les gouvernements ont mis en place des plans alternatifs d'assurance contre les crues garantis par l'état.

En ce qui concerne le secteur financier, les risques liés au changement climatique sont de plus en plus souvent pris en compte pour des secteurs spécifiques susceptibles d'être touchés tels que les projets hydroélectriques, l'irrigation et l'agriculture, ainsi que le tourisme.

Les effets du changement climatique sur le tourisme pourraient être positifs ou négatif, des climats plus chauds ouvrent la possibilité d'extension des environnements exotiques (par exemple, avec la présence de palmiers en Europe occidentale), ce qui pourrait sembler positif à des touristes, mais pourrait entraîner l'extension spatiale et l'amplification de maladies d'origine hydrique et de maladies à vecteur. Les sécheresses et l'extension des environnements arides (et les effets des épisodes météorologiques extrêmes) pourraient décourager les touristes. Les régions qui dépendent de la disponibilité de la neige (notamment pour le tourisme hivernal) font parties des régions les plus vulnérables au changement climatique. Les assurances étendent les risques et contribuent à l'adaptation, et la gestion de fonds d'assurance a des implications pour l'atténuation.

Le réchauffement en 2100	<2°C		3°C	5°C
Répercussions matérielles	1,5°C	2°C		
Élévation du niveau des océans (cm)	0,3 à 0,6 m	0,4 à 0,8 m	0,4 à 0,9 m	0,5 à 1,7 m
Structures côtières à protéger (T$)	10,2 T$	11,7 T$	14,6 T$	27,5 T$
Probabilité d'étés sans glaces en Arctique	1 sur 30	1 sur 6	4 sur 6 (63 %)	6 sur 6 (100 %)
Cyclones tropicaux : Moins (force 1-5)	-1 %	-6 %	-16 %	Inconnu
Plus fort (force 4-5)	+24 %*	+16 %	+28 %	+55 %
Plus humide (précipitations totales)	+6 %	+12 %	+18 %	+35 %
Fréquence des pluies extrêmes	+17 %	+36 %	+70 %	+150 %
Augmentation des feux de forêt	x1,4	x1,6	x2,0	x2,6
Vagues de chaleur extrêmes	x22	x27	x80	x300
Surface terrestre propice à la malaria	+12 %	+18 %	+29 %	+46 %
Répercussions économiques				
Effet sur le PIB mondial (2018 : 80 T$)	-10 %	-13 %	-23 %	-45 %
Actifs inutilisables	Transition : combustible fossile (approvisionnement, production, transport, industrie)		Mitigés : certains actifs liés au combustible fossile mis au rancart, certain niveau d'inutilisation	Matérielles : zones inhabitables, agriculture, secteurs tributaires de l'eau, pertes touristiques, etc.
Approvisionnement alimentaire	Régime alimentaire, perte de rendement dans les tropiques		Perte de rendement de 24 %	Perte de rendement de 60 %/ hausse de la demande de 60 %
Occasions en assurance	Nouveaux investissements dans les actifs et l'infrastructure à faibles émissions de carbone (p.ex. CSC)		Augmentation de la demande pour gérer la hausse des risques	Minimes : récession, tensions, risques élevés et imprévisibles

Figure 1 : Impact des scénarios de réchauffement d'ici 2100.

Source : CRO Forum, 2019, page 5. Reproduit avec autorisation.

Faire face aux risques liés aux changements climatique :

Les incidences économiques du changement climatique à l'échelle mondiale sont difficiles à estimer. En effet, le changement climatique aggrave et augmente la fréquence des catastrophes naturelles, à ce titre, ce sont les segments les plus vulnérables de la population qui sont les plus touchés.

L'assurance, en tant que part intrinsèque de la gestion des risques, joue un rôle capital dans le renforcement de la résilience et de la protection des individus et des communautés contre les catastrophes naturelles.

L'environnement réglementaire et de supervision contribue énormément à la mise en place de moyens et de mécanismes novateurs dans la réduction de l'écart de protection en matière d'assurance climatique.

Les régulateurs sont ainsi bien placés pour stimuler les mesures susceptibles de renforcer la résilience face aux risques climatiques à travers l'instauration d'assurance obligatoire des catastrophes naturelles pour les particuliers et les industriels.

Particulièrement, les opérateurs du secteur de l'assurance sont de plus en plus conscients de l'importance de la quantification et de la divulgation des répercussions financières des changements climatiques relativement à cet objectif.

Les effets des changements climatiques, en particulier les phénomènes météorologiques extrêmes et leurs répercussions, ont influé et continuent d'influer sur le travail des actuaires en assurances IARD. Les assureurs devront tenir compte de la façon dont ils couvrent les risques découlant d'événements météorologiques extrêmes et utiliser de meilleurs modèles et de meilleures données.

Des actions multiples de tous ces acteurs : sociétés d'assurance et de réassurance, superviseur, associations d'actuaires œuvrent à faire bouger les choses notamment :

- Prioriser la collecte de données liées aux répercussions financières des événements climatiques : plusieurs associations et groupes de réflexions ont lancé des appels aux gouvernement pour superviser la collecte et la divulgation de données nationales sur les répercussions financières des événements climatiques, comme les inondations, les tempêtes de vent et les feux de forêt et de rendre obligatoire la divulgation financière des risques et des possibilités liés au climat.

- Mettre en œuvre des politiques pour accélérer l'application d'exigences de rapports financiers liés aux risques climatiques ;

- Tenir compte des facteurs environnementaux dans les décisions de placement et la planification des risques en entreprise : ces critères aident à mesurer la viabilité et l'impact éthique des placements et des souscriptions au-delà des risques financiers évidents. L'exemple du charbon est révélateur du changement de comportement des assureurs, en effet, à mesure que le monde se dirigent vers des sources d'énergie à faibles émissions de carbone, certaines réserves mondiales de combustibles fossiles pourraient ne jamais être exploitées, le charbon, par exemple, a perdu la faveur des assureurs, nombre d'entre eux ayant réduit ou éliminé l'assurance ou leur participation dans les entreprises qui tirent leurs revenus du charbon.

Ces mesures importantes aideront à gérer les répercussions financières associées aux risques climatiques auxquels les entreprises sont confrontées et à garantir la sécurité financière adaptée aux changements climatiques.

Par ailleurs, le Groupe de travail sur l'information financière relative aux changements climatiques (TCFD Task Force on Climate-related Financial Disclosures), mis sur pied par le Conseil de stabilité financière (FSB) afin d'élaborer un ensemble uniforme d'informations à fournir sur une base volontaire relativement aux risques financiers liés aux changements climatiques dont les entreprises

pourront se servir pour présenter des informations aux créanciers, aux assureurs, aux investisseurs et aux autres parties prenantes, a publié les recommandations sur la divulgation efficace des risques financiers liés aux changements climatiques.

Les quatre recommandations faciles à adopter au sujet de l'information financière relative aux changements climatiques s'appliquant aux entreprises issues de différents secteurs et territoires ont reçu un énorme soutien et demeurent inchangées :

Gouvernance : Fournir de l'information sur la gouvernance de l'organisation à l'égard des occasions et des risques liés aux changements climatiques.

Stratégie : Fournir de l'information sur les répercussions réelles et potentielles des occasions et des risques liés aux changements climatiques sur les activités, la stratégie et la planification financière de l'organisation.

Gestion des risques : Fournir de l'information sur la façon dont l'organisation identifie, évalue et gère les risques liés aux changements climatiques.

Mesures et cibles : Fournir de l'information sur les mesures et les cibles utilisées pour évaluer et gérer les occasions et les risques liés aux changements climatiques pertinents. Les informations supplémentaires suivantes sont disponibles sur le site du FSB :

Les recommandations se distinguent essentiellement par le fait qu'elles sont faciles à adopter par l'ensemble des organisations, qu'elles doivent être incluses dans les principaux documents financiers, qu'elles ont été conçues pour faciliter la présentation d'informations prospectives utiles à la prise de décision au sujet de l'incidence financière et qu'elles sont surtout axées sur les risques et les occasions liés au virage vers une économie à faible émission de carbone.

Le TCFD recommande également la divulgation des répercussions potentielles des occasions et des risques liés aux changements climatiques selon différents scénarios possibles, par exemple un scénario où le réchauffement est de 2 °C.

Risques Emergents

2. L'évolution des risques pandémiques

Il est complexe d'établir une classification précise des risques émergents, car les catégories identifiées de risques ont des contours flous qui parfois se chevauchent. Dès lors, il est plus solide de classifier les risques émergents plutôt selon leurs facteurs d'apparition que par leurs conséquences. Un risque émergent lié à la santé peut trouver sa cause dans plusieurs facteurs. Les débats récurrents sur la multifactorialité des risques pandémiques en sont une illustration.

Les risques de pandémie sont émergents du fait qu'ils soient à la fois nouveaux et croissants. Nouveau signifie que le risque n'existait pas auparavant ou récemment découvert en raison de nouvelles connaissances scientifiques ou de nouvelles perceptions par le public. Et Croissant du fait que le nombre de causes du risque est croissant, la probabilité d'y être exposé est croissante ou l'effet du risque sur la santé empire.

Un défi en ce qui concerne les risques émergents est qu'ils sont connus dans une certaine mesure, mais ne sont pas susceptibles de se matérialiser ou d'avoir un impact avant plusieurs années. Un risque émergent commence lentement comme une méga tendance ou une innovation, mais ce démarrage lent peut potentiellement avoir un impact très important sur le long terme. Et c'est exactement le cas pour les risques de pandémies.

En 2020, le risque d'une pandémie mondiale est devenu réalité. La pandémie COVID-19 a enseigné au monde, qui devient de plus en plus attentif aux risques, des leçons de risque et de résilience. La pandémie a choqué les populations du monde entier avec une ampleur sans précédent dans l'histoire récente. Bien que les circonstances puissent être uniques, la réalité est qu'il y aura plus de catastrophes inattendues dans un proche avenir.

Les pandémies vont augmenter en fréquence et en gravité

Ce qui était autrefois des événements une fois tous les cent ans, comme des saisons record d'ouragans et d'incendies de forêt, nous frappent maintenant tous les cinq ans environ. Il s'agit d'un moment critique pour adopter une vision holistique du risque afin de se préparer aux catastrophes à grande échelle à venir.

Plusieurs facteurs conduisent à un accroissement du risque pandémique. Nous sommes aujourd'hui dans une situation pour le moins paradoxale : les risques pandémique diminuent, voire sont éradiqués pour certaines maladies, mais l'apparition de nouvelles épidémies/pandémies est un fait et des maladies connues génèrent de nouvelles problématiques.

Bien que ce risque varie considérablement selon la zone géographique, le mode de vie moderne et le développement des transports et des migrations peuvent entraîner une propagation rapide et massive de maladies infectieuses pour devenir d'ampleur planétaire.

L'effet des migrations sur les épidémies a été illustré historiquement lors de la conquête de l'Amérique latine par les conquistadors. Les populations indiennes ont été décimées par des virus amenés par le conquérant, par exemple la rougeole et la variole. En sens inverse, les conquérants ont ramené en Europe des maladies telles que la syphilis.

Par ailleurs, l'UNESCO a fortement soutenu la théorie de la Plateforme intergouvernementale scientifique et politique sur la biodiversité et les services écosystémiques (IPBES) qui établit les liens

entre la perte de biodiversité et l'augmentation des facteurs de risque de pandémie. Selon l'IPBES, il existe un lien évident entre les pandémies sanitaires mondiales et la crise de la biodiversité et climatique. Les causes profondes des pandémies sont également le moteur de l'érosion de la biodiversité et du changement climatique : les activités humaines.

Les changements d'affectation des terres, l'expansion et l'intensification de l'agriculture ainsi que le commerce et la consommation d'espèces sauvages perturbent les écosystèmes, favorisent une proximité entre les humains et les animaux sauvages, le bétail et les hommes et de ce fait avec les agents pathogènes qu'ils transportent.

Le rapport avertit que les futures pandémies apparaîtront plus souvent, se propageront plus rapidement, feront plus de dégâts à l'économie mondiale et tueront plus de personnes que la COVID-19, à moins que l'approche globale de la lutte contre les maladies infectieuses ne change, passant de la réaction à la prévention. Les experts estiment que le coût de réduction des risques pour prévenir les pandémies est 100 fois moins élevé que le coût de la réponse à ces pandémies, «fournissant donc de fortes incitations économiques pour un changement transformateur». Cela nécessitera une réévaluation et une transformation profondes de la relation entre l'humain et la nature, ainsi que des pratiques de consommation non durables qui entraînent la perte de biodiversité, le changement climatique et l'émergence de pandémies.

Les experts recommandent l'établissement d'un nouveau partenariat intergouvernemental en matière de santé et de commerce, et la création d'un conseil intergouvernemental de haut niveau sur la prévention des pandémies.

Ainsi, le risque épidémique est universel et tous les pays sont donc confrontés à des facteurs d'accroissement du risque épidémique endogènes et exogènes, dont :

1. Les conditions de vie

La forte chute de la mortalité liée aux épidémies au cours du vingtième siècle résulte d'abord de l'amélioration de l'hygiène qui a eu un impact supérieur au progrès de la médecine.

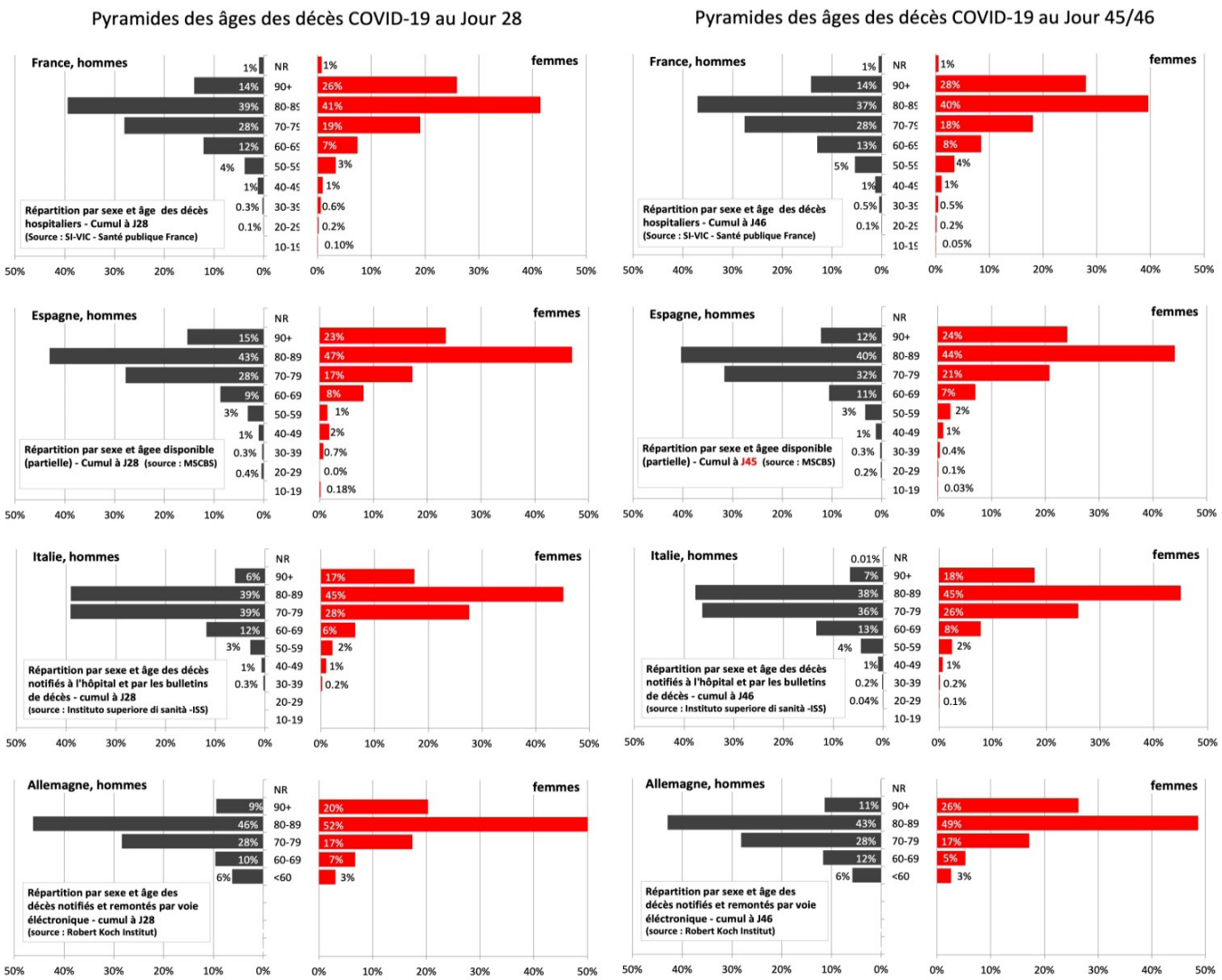
Paradoxalement, aujourd'hui, les populations ont tendance à abandonner des règles élémentaires d'hygiène tout en exigeant, en particulier dans le domaine de l'alimentation, des produits de plus en plus aseptisés qui peuvent les fragiliser.

Une autre source de propagation des pandémies repérée est l'accroissement de la pollution de l'air dans les villes.

2. L'âge

La vulnérabilité de la population des pays occidentaux s'accroît également du fait du vieillissement de la population car les défenses immunitaires déclinent avec l'âge. Certaines maladies infectieuses touchent de ce fait beaucoup plus durement les personnes âgées.

La part grandissante des personnes âgées dans les sociétés, implique la présence d'un nombre croissant de personnes plus fragiles devant les maladies infectieuses. Covid-19 a dramatiquement illustré cette donnée, plus on monte en âge, plus la mortalité augmente. D'ailleurs, plus de 90 % des décès du Covid-19 surviennent chez les plus de 65 ans et l'âge moyen des victimes du Covid est de 82 ans et la moitié des morts ont plus de 85 ans.



Citation. Graphique tiré de « La démographie des décès par COVID-19 (2020). Institut national d'études démographiques (Ined). Extrait de : https://dc-covid.site.ined.fr/fr/ »

3. L'urbanisation

L'accroissement de la population urbaine constitue historiquement le principal facteur ayant permis la propagation des épidémies. La majorité des épidémies se sont propagées par le non-respect des règles de quarantaine et ensuite par les échanges commerciaux.

De ce fait, très tôt, ceux qui le pouvaient, cherchaient à se réfugier à la campagne. Bien que l'épidémie débutât souvent dans les quartiers portuaires pauvres et insalubres, on réalisa très vite que la mort frappait sans distinction sociale ou sexuelle. Et qu'en conséquence, l'isolement à la campagne était l'unique protection.

Aujourd'hui, ce n'est pas tant l'urbanisation que les conséquences de l'organisation sociale des grandes cités, avec la nécessité de prendre des transports en commun et la promiscuité pouvant en résulter aux heures de pointe, qui sont facteurs de diffusion des épidémies. La surveillance rigoureuse des réseaux de distribution d'eau est également facteur de prévention en permanence.

4. L'importance des migrations

La peste noire, arrivée d'Asie par les routes de la soie maritimes et terrestres, est réputée avoir exterminé la moitié de la population européenne, soit entre 20 et 30 millions de personnes. Ceci nous rappelle que les déplacements humains sont les vecteurs naturels des épidémies et par là de tentations xénophobes.

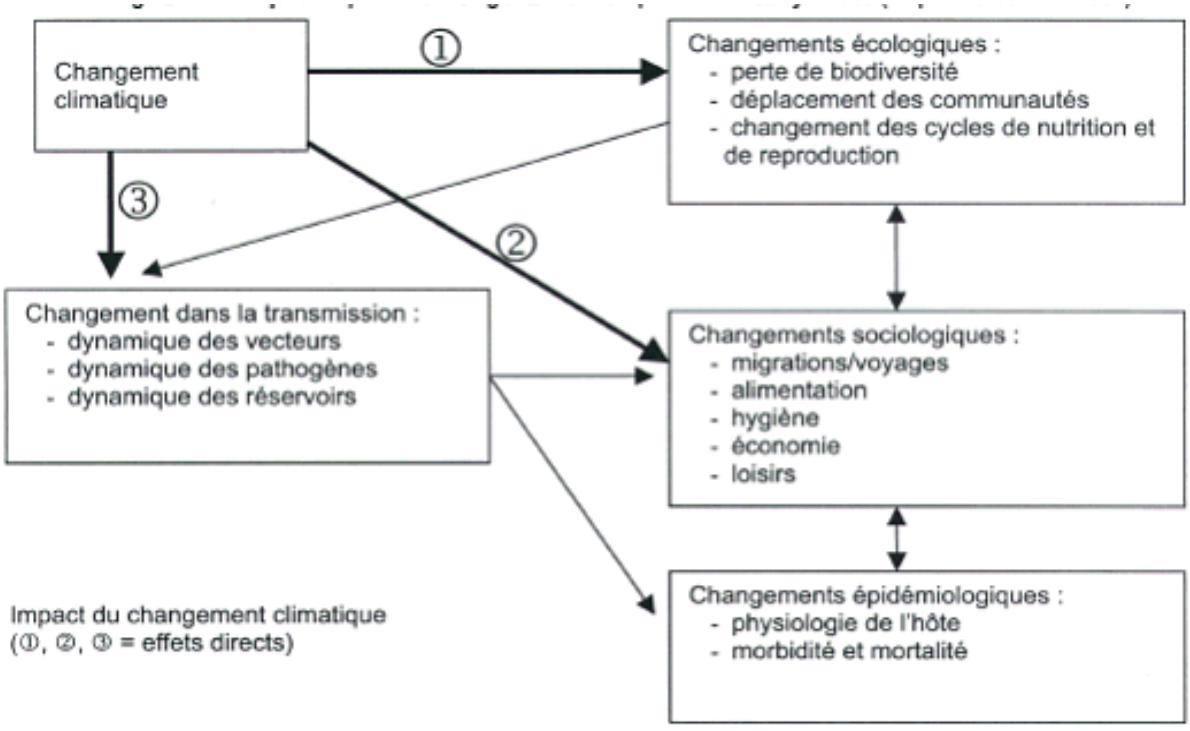
La propagation des maladies infectieuses par les transports est aujourd'hui une donnée permanente du monde et des méthodes efficaces pour enrayer les épidémies, telles l'autarcie et la quarantaine, sont aujourd'hui difficilement praticables. Or, la peste de 1347 est passée directement de Bordeaux à Londres par le commerce du vin, avec une escale à Rouen, grâce à laquelle elle est remontée via la Seine jusqu'à Paris.

Les microbes ne connaissent pas les frontières, ils voyagent avec les avions, de façon extrêmement rapide. Ils ne sont d'ailleurs pas les seuls à voyager puisque la résistance aux antibiotiques voyage également à grande vitesse et, lorsqu'un nouvel antibiotique est créé, nous voyons la résistance apparaître en un lieu et se propager en quelques semaines dans d'autres pays de la planète. Les échanges sont aujourd'hui, à l'évidence, le principal vecteur de diffusion des épidémies et en tous cas de la rapidité de propagation. Covid-19 en est l'exemple parfait.

5. Le réchauffement climatique

S'agissant généralement de maladies infectieuses, la propagation des épidémies est étroitement liée à la notion de réchauffement climatique. Par exemple la fièvre catarrhale ovine, propagée par un petit diptère, a beaucoup progressé ces dernières années sur le pourtour méditerranéen. Or, une augmentation de 1° centigrade de la température moyenne permet à l'insecte vecteur de cette maladie d'accroître son aire de répartition de 90 en latitude et de 150 m en altitude ce qui est suffisant pour permettre à l'épidémie de se propager sur tout le bassin méditerranéen.

Un autre exemple est donné par la fièvre du Nil occidental (West Nile) qui a envahi tous les États-Unis en quelques mois avec quelques épisodes en Europe. C'est un Culicoides qui est responsable de cette transmission, il remonte vers le Nord à la faveur du réchauffement climatique.



Impact du changement climatique
(①, ②, ③ = effets directs)

6. L'évolution des comportements humains et des modes d'alimentation

Longtemps nous avons cru que l'homme était protégé des virus des animaux par la notion de barrière d'espèce.

Il est maintenant avéré que des modifications dans le cycle de multiplication d'un virus peuvent conduire à des réplications pouvant passer d'une espèce à l'autre, en particulier de l'animal à l'homme.

Certains virus qui, à l'état naturel, sont incapables d'infecter l'homme lors d'un contact direct avec des animaux infectés ou un environnement souillé peuvent représenter un danger lors de l'utilisation de produits médicamenteux d'origine animale. Par ailleurs de nouvelles maladies infectieuses peuvent émerger suite à l'introduction d'un nouvel agent pathogène ou l'adaptation d'un agent existant ou à une modification dans les pratiques d'élevage.
L'exemple le plus documenté est l'apparition du virus de Hong Kong en 1968. Ce nouveau virus s'est rapidement étendu aux pays voisins puis au monde entier en l'espace d'une année. Les virus humains qui circulaient seuls depuis 1957 appartenaient au sous-type A (H2N2). Deux gènes dont un gène majeur ont alors été remplacés par leurs équivalents de virus aviaires : H3 a remplacé H2.
Les pandémies de grippe prennent souvent naissance en Extrême-Orient où la population très dense vit en contact étroit avec les animaux
Toutefois les conditions diffèrent entre le reste du monde et l'Asie du Sud-Est où l'augmentation rapide de la densité des petits élevages liée à la proximité sur un même territoire d'élevages de porcs et de poulets, crée un environnement favorable à la grippe aviaire.
Ce mouvement se constate notamment en Asie du Sud-Est où se sont développés le SRAS, l'influenza aviaire et, peut-être, en Afrique avec l'Ebola, liée à des nouveaux commerces, à des nouveaux marchés où l'on trouve un grand nombre d'animaux, des espèces différentes sur le même lieu et, bien entendu, une forte concentration humaine.
Un autre facteur particulièrement important réside dans les mouvements illégaux ou incontrôlés d'animaux et de produits d'origine animale tels que :

✓ le trafic d'espèces protégées et l'insuffisance patente des contrôles vétérinaires pour les animaleries peuvent être à l'origine d'importations de maladies tropicales.
✓ Les fêtes religieuses imposant le sacrifice d'animaux peuvent, lorsque l'abattage se fait en dehors de tout contrôle sanitaire.
✓ La fièvre aphteuse, qui s'est développée au Royaume-Uni en 2001, trouve son origine dans les eaux grasses (déchets de cuisine) d'un restaurant asiatique qui ont été données à un élevage de porc qui a ensuite contaminé tout le pays et une grande partie de l'Europe.
✓ Enfin, en cas de contamination non déclarée, les transports d'animaux vivants, comme la diffusion d'aliments frelatés sont facteurs d'extension de l'épidémie.

Ces dernières années Les progrès enregistrés ont été particulièrement spectaculaires en termes de rapidité d'identification de l'origine des sources d'épidémies. Toutefois, la difficulté majeure réside dans l'identification précoce de l'épidémie.

Modélisation des risques pandémiques

Une pandémie désigne littéralement une maladie qui affecte « le peuple tout entier ». De par l'ampleur qu'il peut prendre, un assureur ne peut se permettre d'ignorer ce risque. Mais celui-ci est particulièrement difficile à évaluer en raison du faible nombre de données disponibles et des nombreuses inconnues qui subsistent quant à la forme que pourrait prendre la prochaine pandémie.

Différents modèles et prédictions existent, mais deux grandes catégories de modèles existent pour évaluer l'impact d'une pandémie : les modèles actuariels, basés sur données historiques, et les modèles épidémiologiques, qui simulent la propagation de la maladie.

Pour les premiers stades des épidémies, les modèles stochastiques, c'est-à-dire basés sur le hasard, sont privilégiés. En effet, un petit groupe de personnes porteuses contamine les gens de manière très aléatoire. À partir d'un certain moment, la loi des grands nombres prend le dessus : on peut alors considérer que le taux de contamination est le même pour tout le monde. Les chercheurs se

tournent alors vers des modèles déterministes, qui permettent de prévoir l'apparition des pics et de jauger les différentes stratégies de contrôle. Typiquement, les modèles individu-centrés sont stochastiques, tandis que ceux populationnels sont, en moyenne, plus déterministes.

Les modèles aident aussi à mieux comprendre le virus. En comparant les prédictions aux statistiques du terrain, les scientifiques repèrent les paramètres qui expliquent les éventuelles différences. Ils en tirent des informations qui leur échapperaient et affinent leurs modèles.

Et c'est sur ces modèles que se basent les dispositifs de risk management CRD4 et Solvabilité 2.

Comme était le cas avec les modèles mis en œuvre après la crise financière 2008-2010, qui constituent actuellement des coussins de fonds propres contra-cyclique et visent à prévenir une situation d'insolvabilité d'une compagnie d'assurance, face à une crise boursière, un risque souverain ou une accélération de facteurs de risques.

Swiss Re suppose que les pandémies se produisent tous les 30 ans et la probabilité annuelle de survenance d'une pandémie est donc estimée à 3,33%. Dans la logique de quantification des risques de Solvabilité 2, il faut donc sélectionner les pandémies dont la gravité se situe sur le quantile 99,5%, ce qui revient à retenir le quantile 85% pour une pandémie dont la probabilité de survenance est de 3,33%.

Il s'agit à présent de spécifier la nature de l'incertitude que l'on souhaite intégrer dans le modèle. Différentes approches peuvent être envisagées.

Les assureurs et réassureurs s'organisent pour apporter des solutions

La nature du risque de pandémie est l'une des raisons pour lesquelles il est jusque-là exclu de la couverture d'assurance. Il est difficile qu'un risque de cette nature soit géré exclusivement par les assureurs, en particulier étant donné l'incapacité de diversifier le risque, du fait qu'il affecte toutes les lignes et toutes les régions et qu'il s'agit d'une situation permanente. C'est ce qui met en doute qu'une éventuelle solution purement assurantielle contre le risque pandémique pourrait être souscrite de manière rentable aux assureurs. Actuellement, le secteur de l'assurance ne peut jouer qu'un rôle limité en raison des contraintes de capacités et de la nature systémique du risque.

En effet, l'industrie modélisait la pandémie depuis un certain temps; c'est un domaine d'expertise où les professionnels de l'assurance pourraient aider à mesurer le risque et à trouver une solution uniquement pour ce qui est dommages IARD. Sur ce plan, le secteur des assurances dispose d'une expertise technique qu'il pourrait apporter pour faire face aux futures pandémies (expérience de gestion des risques et l'évaluation des sinistres…) mais les pertes financières seraient mieux couvertes par des partenariats public-privé. La mise en œuvre du partenariat doit avoir lieu au niveau mondial et ensuite adaptée aux différents pays, car les lois visant à amortir les effets d'une pandémie diffèrent d'un pays à l'autre.

Dans ce partenariat public-privé, le rôle des assureurs serait principalement :

- **Mieux comprendre leurs risques critiques**. Le COVID-19 a clairement montré que de nombreuses entreprises n'avaient pas pleinement envisagé les effets qu'une épidémie ou une pandémie pouvait avoir sur leurs personnes et leurs opérations, leurs infrastructures essentielles et leurs gouvernements. Un investissement accru dans la collecte de données et les outils de modélisation peut aider les assureurs, les courtiers et les entreprises à anticiper et à quantifier les risques potentiels.
- **Offrir une couverture d'assurance pour répondre à des besoins uniques**. Idéalement, les assureurs n'offriront pas de solutions de couverture uniformes. Les assurés potentiels devraient être en mesure de personnaliser les polices d'assurance contre la pandémie qu'ils souscrivent - par exemple, en sélectionnant des risques de maladies infectieuses spécifiques à assurer et en ajustant les limites pour répondre à leur tolérance au risque et à d'autres préférences.

• **Adopter des pratiques pour éviter les pertes liées à la pandémie**. Les preneurs d'assurances cherchent à atténuer la valeur de leurs biens, exposition aux accidents de travail et les cyber-risques auxquels ils sont exposés, grâce à des techniques de construction en hauteur, des programmes de sécurité au travail et des programmes de cybersécurité. Les assureurs récompensent les assurés qui peuvent démontrer leur engagement envers de tels processus sous la forme de tarifs et conditions plus favorables. Un programme d'assurance contre les risques de pandémie financé par le gouvernement qui encourage l'amélioration des pratiques de santé et de sécurité peut produire des avantages similaires.

Par ailleurs et face à la réalité du COVID-19 et la demande immense de couvertures en assurance des pandémies, les assureurs ont su qu'ils peuvent faire beaucoup plus pour soutenir leurs clients en les protégeant contre les risques changeants auxquels ils sont confrontés. Ainis, des travaux en vue de la création d'un futur dispositif assurantiel des « risques exceptionnels » ont été lancés avec pour objectif : bâtir rapidement une solution pour faire face à toute crise semblable à celle du Covid-19. Certains produits d'assurance ont été développés pour offrir une couverture explicite pour les pertes liées à une interruption d'activité subies à la suite d'une épidémie, soit en tant que police autonome spécialisée, soit en tant qu'avenant à la couverture d'interruption d'activité existante d'un titulaire de police.

Marsh, en partenariat avec Metabiota et Munich Re, a créé une solution d'assurance d'atténuation des risques pour l'industrie de la vente au détail, de gros, de l'alimentation et des boissons qui offre une protection financière contre les retombées d'une pandémie ou d'une épidémie. En utilisant des déclencheurs tels que l'indice de sentiment pathogène de Metabiota et d'autres, les entreprises de vente au détail, de gros, d'alimentation et de boissons peuvent désormais mieux comprendre le risque de perturbation opérationnelle posé par une épidémie ou une pandémie et assurer leur risque.

Aussi, Lloyds a conçu une solution potentielle d'interruption d'activité sans dommage, ReStart pour aider en particulier les petites et moyennes entreprises. La solution vise à donner la certitude d'une couverture d'interruption d'activité sans dommages dans un premier temps aux PME britanniques en mettant en commun des capacités limitées entre un certain nombre d'acteurs du marché de la Lloyd's. Le produit soutiendrait la réouverture des PME, en offrant une gamme de limites garantissant que la couverture est abordable pour les clients sans nécessiter de soutien gouvernemental. C'est une solution pour les futures vagues de COVID-19.

Recover Re, présente une proposition de produit d'assurance «après l'événement». L'intention ici est de fournir un soulagement immédiat et une couverture en cas d'interruption d'activité sans dommage à long terme, y compris la pandémie actuelle de COVID-19. Cela pourrait être un moyen efficace d'injecter des fonds commerciaux et gouvernementaux dans l'économie. Ce dispositif pourrait être mis en œuvre dans n'importe quel pays où le gouvernement dispose des ressources et de l'engagement de l'industrie pour le soutenir.

Le réassureur Black Swan Re a également apporté sa solution de réassurance par le biais d'un capital mis en commun par le secteur et soutenu par une garantie du gouvernement de payer si jamais le pool avait des fonds insuffisants. Cette solution pourrait contribuer à mieux protéger les clients contre les effets à long terme d'événements catastrophiques systémiques d'une autre pandémie, ou d'une interruption de la chaîne d'approvisionnement mondiale, de l'interruption d'infrastructures ou de services publics critiques.

Risques liés au Covid-19, à observer à partir de 2021

Alors, à quoi les organisations devraient-elles être prêtes à faire face en 2021? Voici quelques tendances à surveiller:

Augmentation du cyber risque. L'un des défis les plus notables à prendre en compte est la possibilité d'une cyber-pandémie mondiale qui coupe Internet ou paralyse considérablement la bande passante. Avec plus de personnes travaillant à distance grâce au COVID-19 ainsi qu'un monde de plus en plus connecté aux appareils de l'Internet des objets (IoT), la technologie est plus critique que jamais. Notre dépendance aux données et à la communication ne fait que croître. Une perturbation massive entraînerait des pertes financières et des dommages collatéraux importants en termes d'interruption d'activité, d'atteinte à la réputation, de responsabilité et de contrôle réglementaire accru.

Développer la résilience d'une organisation face à tout événement cybernétique majeur sera essentiel à l'avenir. Cela comprend la cyber-assurance ainsi qu'une analyse approfondie de la planification des contingences et de la continuité des activités, de l'infrastructure, de la formation des employés et de la gestion de crise post-événement. Alors que de nombreuses organisations ont fait la transition de leur main-d'œuvre vers un modèle de travail à distance, le cyber-risque devient de plus en plus complexe. Même avant le COVID-19, le marché de la cyber-assurance adoptait déjà une vision plus proactive du risque et continuera d'être un élément évolutif et obligatoire de la gestion des risques en 2021.

Modèles alternatifs de couverture des risques. Alors que les primes d'assurance continuent d'augmenter dans tous les secteurs, les entreprises sont obligées de prendre des décisions difficiles quant au niveau de risque qu'elles souhaitent conserver par rapport au montant de risque qu'elles souhaitent transférer aux assureurs. Les captives sont de plus en plus attractives en tant que modèle de couverture des risques car elles ne sont pas soumises aux hauts et aux bas du marché dur et mou. Il y a un intérêt croissant pour l'éventail complet des captifs, du payeur unique aux captifs de groupe en passant par le 831 (b) s, et cette tendance se poursuivra probablement.

De plus en plus d'assurés recherchent également des captives pour réduire certains des coûts de friction liés à l'échange de dollars avec les compagnies d'assurance. Les organisations qui envisagent cette option devront comprendre les avantages et les inconvénients d'une captive et si cela a du sens pour eux. Les courtiers et les professionnels du risque qui peuvent évaluer la faisabilité de la captive et guider les entreprises tout au long du processus de la création à la gestion d'une captive auront un avantage stratégique.

Changement climatique. Il ne fait aucun doute que les événements météorologiques sont de plus en plus violents et fréquents. Les phénomènes catastrophiques s'étendent dans des zones qui étaient autrefois considérées comme sûres. Le surdéveloppement autour des zones côtières a mis en péril des milliards, voire des billions de dollars immobiliers. Avec l'élévation du niveau de la mer, les ouragans, les incendies de forêt et les tempêtes de vent, aucune partie des États-Unis n'est à l'abri du changement climatique.

Du point de vue de l'assurance, le changement climatique a un impact énorme sur la tarification et le montant des risques que les assureurs sont prêts à absorber. Elle les pousse à réévaluer leurs modèles autour des sinistres, primes et pertes protégées. En conséquence, nous constatons une baisse de la capacité qu'ils sont prêts à écrire.

Dans le paysage changeant de l'assurabilité, comment les organisations peuvent-elles s'assurer d'avoir une assurance efficace en place? Les entreprises doivent repenser et repenser les structures et les méthodes pour atténuer les pertes dues aux événements météorologiques. La mise en œuvre d'une stratégie de risque efficace comprend une gamme beaucoup plus large de mesures holistiques telles que le déplacement des systèmes mécaniques, l'utilisation d'espèces végétales ignifuges dans l'aménagement paysager, la création de talus et l'intégration de programmes d'entretien efficaces.

Une discipline de souscription plus stricte. En fin de compte, le changement climatique a un impact sur la façon dont les assureurs considèrent le risque. Surtout dans ce marché qui se durcit, alors que les capacités diminuent et que les primes augmentent, les assureurs sont très attentifs à la qualité du risque. Un examen plus approfondi sera exercé sur les entreprises pour montrer, par exemple, que les recommandations d'ingénierie sont satisfaites et qu'elles complètent les services de contrôle des sinistres offerts par les compagnies d'assurance.

Pour aggraver les choses, les souscripteurs d'assurance sont inondés de soumissions. Lorsqu'un souscripteur examine 50 soumissions, avoir une soumission de qualité, le risque de qualité et le courtier de qualité sont importants. Arriver au sommet en termes de garantie de la meilleure couverture et de la tarification deviendra de plus en plus difficile. Les assurés devront démontrer qu'ils représentent un risque impérieux et qu'ils ont mis en place une gestion proactive des risques. La discipline de souscription est de retour avec une vengeance et c'est une tendance qui se poursuivra probablement dans un avenir prévisible.

Des marchés plus durs. Avant le COVID-19, le marché était déjà difficile, en particulier dans les secteurs de l'automobile, des biens / dommages et des excédents de responsabilité. Toutes les industries ont été touchées par cette pandémie. Dans les segments durement touchés tels que le divertissement, les soins de santé et l'hôtellerie, il deviendra encore plus difficile de placer des risques à mesure que la capacité diminuera et que les tarifs augmenteront. Le marché difficile est là dans un avenir prévisible, et COVID ne fera que le prolonger et incitera des conditions plus restrictives.

Jusqu'à récemment, la seule ligne qui avait été relativement épargnée par le marché dur était l'indemnisation des travailleurs. Cependant, la réduction des revenus de placement sur les primes des compagnies d'assurance, ainsi que les modifications législatives découlant du projet de loi 5 de l'Assemblée de la Californie, imposant une couverture d'indemnisation des travailleurs pour certains entrepreneurs indépendants, accentueront le stress sur le marché, qui devrait encore se durcir en 2021.

Compte tenu de la pandémie en cours, des conditions difficiles du marché et des menaces posées par le changement climatique, une bonne gestion des risques est primordiale pour le succès et la survie d'une organisation. Il ne s'agit plus de risque générique. Les assurés et les courtiers doivent comprendre la nature de leur industrie et de leur gamme de produits spécifiques. Pour aller de l'avant en ces temps difficiles, il sera de plus en plus important d'avoir une concentration et une expertise accrues dans les domaines de spécialité.

Conclusion

Alors que les gouvernements, les entreprises et les assureurs examinent les dégâts infligés au cours de l'année écoulée, il est plus important que jamais de renforcer la prospective stratégique, non seulement comme une tâche essentielle de se préparer à la prochaine pandémie, mais aussi de jouer un rôle plus actif dans les risques mondiaux.
Pour être à la hauteur de leurs ambitions d'être plus durable, les assureurs et réassureurs doivent anticiper plutôt que simplement réagir.

La prochaine crise mondiale est un scénario très réaliste et peut être déclenchée par une cyberattaque mondiale, ou une catastrophe Naturelle à grande échelle due au changement climatique. Les deux risques sont systémiques et ne peuvent pas être gérés par les assureurs seuls. Ce dont le monde a besoin, est une approche globale de partenariat entre le secteur de l'assurance, les entreprises et les gouvernements.

Risques Emergents

3. Cyber-risque

Les risques technologiques sont très bien classés dans plusieurs revues industrielles traitant des risques émergents. Selon les gestionnaires des risques de l'industrie, il s'agit de la catégorie de risques qui consomme le plus de temps et de ressources. Ils estiment que les risques technologiques auront un impact financier important sur leurs organisations et que des solutions d'assurance sophistiquées sont de la plus haute importance.

Parmi ces risques technologiques, le cyber-risque est devenu le risque majeur pour les assureurs et réassureurs pour les 5 prochaines années, tant en probabilité d'occurrence qu'en impact. En effet, l'intensification des cyber-attaques, la multiplication de leurs formes et l'augmentation de la vulnérabilité accroit la gravité de ce risque.

Cyber risque / Cyber-attaques :

Le développement des technologies de l'information et de la connectivité en ligne, le traitement médiatique de l'information, l'hyper-transparence à l'égard des consommateurs ont changé le mode de fonctionnement des entreprises. Face à la taille importante des données, les systèmes informatiques complexes sont essentiels à l'économie d'aujourd'hui. À ce titre, nous examinons les risques associés avec la cyber-technologie comme exemple du domaine des «risques technologiques» émergents.

Les cyber-attaques de toutes sortes sont désormais au cœur des préoccupations des gouvernements, des services publics, des particuliers, des médecins, des universitaires et des institutions et entreprises de toutes tailles. En raison de l'interconnexion mondiale croissante et de l'utilisation explosive des appareils mobiles et médias sociaux, le risque de cyber-attaques et de violations de données a augmenté de façon exponentielle. Les pirates peuvent fermer le réseau d'une entreprise ou voler les informations personnelles et financières des clients et des employés.

Les cyber-attaques sont désormais considérées comme l'un des plus graves défis de sécurité nationale auxquels sont actuellement confrontés les gouvernements du monde entier.

Certains des risques auxquels les entités sont confrontées dans ce domaine comprennent :

- La Responsabilité juridique
- Les Failles de sécurité informatique
- La Violation de la vie privée
- Le Cyber-vol
- Le Cyber-espionnage
- La Cyber- extorsion
- Le Cyber-terrorisme
- La Perte de revenus
- Le Recouvrement des coûts
- Les Dommages à la réputation
- La Continuité des activités / perturbations de la chaîne d'approvisionnement
- Les cyber-menaces sur l'infrastructure

Coût des Cyber-attaques :

Les économies ont des niveaux de dépendance élevés et en constante augmentation à l'égard des systèmes informatiques, des applications et des logiciels qui contribuent à l'exposition systémique. La croissance de la connectivité entre les mondes numérique et physique ainsi que les progrès du déploiement commercial de l'Internet des objets et de l'intelligence artificielle se traduiront par de nouveaux vecteurs de cyber-attaques et augmenteront encore les effets d'agrégation des risques.

En effet, une cyber-attaque peut imposer aux entreprises des coûts importants. Par exemple, un cyber-incident peut entraîner une interruption d'activité suite à la défaillance des systèmes d'information et donc des dépenses exceptionnelles et des revenus réduits. Les montants impliqués dépendent du temps nécessaire pour restaurer les systèmes affectés ou mener des enquêtes criminelles.

Il y a d'autres coûts qui en résultent, y compris les dépenses pour les mesures prises pour informer les clients, récupérer les systèmes et données ou améliorer la réputation. Cependant, les pertes de tiers peuvent également être extrêmement coûteuses. Les entreprises peuvent faire face à des recours collectifs et payer des dommages-intérêts aux clients dans des cas de violation de données. Les frais de défense suite aux résultats d'une cyber-attaque peuvent inclure les frais d'avocats pour la défense d'affaires devant les tribunaux, empêchant ainsi les affaires de se saisir des tribunaux et les coûts des analyses juridiques de la situation et des recommandations sur la manière de procéder.

Les violations de données de haut niveau et autres incidents de cyber-sécurité ont de plus en plus de résultats onéreux.

Par ailleurs, les organisations, par leur interconnexion et leur participation dans les chaînes d'approvisionnement mondiales, sont soumises à un réseau de plus en plus complexe. Une cyber-attaque peut mettre l'ensemble de la chaîne d'approvisionnement d'une entité à risque. Les cyber-risques posent un ensemble d'agrégations / accumulations de risques qui s'étendent au-delà de la société aux affiliés, aux sous-traitants, aux contreparties et aux chaînes d'approvisionnement.

L'informatique en nuage est un autre cyber-risque préoccupant : L'agrégation des données de nombreuses entreprises à travers un service cloud peut entraîner des pertes catastrophiques pour de nombreuses entreprises en cas d'attaque ou de violation. Que ce soit un cloud privé utilisant des serveurs dédiés ou un cloud public, où les données sont stockées sur des serveurs partagés, des cyber-menaces existent.

Des réglementations sur la protection des données et les lieux de stockage afin de fournir aux gouvernements un meilleur contrôle sur leurs données sont mises en œuvre dans le monde entier. La justification de ce contrôle est fondée sur des préoccupations en matière de protection de la vie privée, de censure et de lutte contre le terrorisme. Le respect des nouvelles réglementations entraînera probablement des changements opérationnels pour les entreprises.

Cyber Assurance

Les progrès rapides des technologies de l'information au cours de la dernière décennie ont introduit un tout nouvel ensemble d'expositions au risque pour les entreprises qui dépendent de plus en plus des technologies de l'information. En 1997, les premiers produits d'assurance contre les cyber-risques ont commencé à émerger lorsqu'on a commencé à identifier les lacunes des produits traditionnels d'assurance de biens et de responsabilité civile générale. Les programmes autonomes de gestion des risques cyber offrant une couverture de première et de tierce partie ont abordé les menaces posées par la cybercriminalité informatique, les logiciels malveillants et la responsabilité potentielle découlant des violations de la sécurité des informations.

Nous avons parcouru un long chemin depuis 1997. La cybercriminalité mondiale a atteint un niveau de sophistication si élevé qu'elle représente un secteur commercial mondial mature, qui innove continuellement et devient plus efficace. En 2017, on a pu observer une utilisation généralisée de méthodes d'attaques de calibre national par des criminels. Les logiciels malveillants sophistiqués à auto-propagation ont été conçus pour supprimer ou manipuler les données, le matériel et les systèmes physiques, ce qui a provoqué des perturbations commerciales majeures pour les entreprises du monde entier, avec un impact monétaire significatif. Le nombre d'attaques de ransomwares a considérablement augmenté. Un nombre croissant d'attaques qui a un impact qui va au-delà de la cible d'origine avec un large effet domino systémique.

Pour faire face à la cyber-menace mondiale, il est de plus en plus important pour les institutions de cet environnement, gouvernements, autorités réglementaires, forces de l'ordre, professions juridiques et d'audit, communauté politique non gouvernementale, secteur des assurances et autres de coopérer. La défense contre les cyber-risques ne peut être efficace que si ces groupes partagent une compréhension commune de la nature changeante des menaces, de leur importance et de leur interconnexion accrue. S'ils travaillent individuellement et conjointement, ces groupes ont la capacité d'augmenter la cyber-résilience collective. Par conséquent, il est vital que toutes les institutions collaborent et partagent leurs connaissances.

Du point de vue de l'assurance, il n'y a pas de politique standard unique pour couvrir les cyber-risques, car les caractéristiques des cyber-menaces varient considérablement selon les secteurs et les tailles d'entreprise, tandis que les termes et conditions des polices d'assurance peuvent parfois être compliquées. Ainsi, les entreprises doivent avoir une compréhension plus approfondie de leur propre exposition car cela aidera à déterminer le type et le montant approprié de couverture requis en fonction de leurs tolérances au risque. En outre, les organisations doivent être conscientes qu'une police de cyber-assurance n'est que l'un des nombreux outils qui forment une stratégie de gestion d'une cyber-sécurité plus complète.

Aider les organisations à identifier le bon équilibre entre les investissements en cyber-sécurité et le transfert du risque résiduel au moyen de produits d'assurance complets est une tâche clé du secteur de l'assurance.

Le risque de cyber-criminalité concerne toutes les entreprises. L'objectif des assureurs est de comprendre comment les cyber-risques peuvent entraîner des pertes pour leurs clients et pour eux-mêmes. Il ne s'agit pas d'un risque nouveau, mais il reste difficile à souscrire car l'impact d'une cyber-attaque peut varier considérablement, en fonction du degré de malveillance de l'attaque et de la vitesse à laquelle elle est identifiée et rectifiée par l'entreprise cible.

Les assureurs doivent également veiller à ce que leurs propres informations confidentielles et des assurés soient protégées. En effet, les assureurs détiennent des quantités importantes de données personnelles. Ils risquent donc de subir de graves atteintes à leur réputation et à leur argent en cas de cyber-attaque. Les échecs en matière de cybersécurité peuvent avoir un impact sur les opérations, les processus de base et la réputation.

Le cyber-risque offre également des opportunités commerciales importantes pour les assureurs / réassureurs :

Avec la gravité et la fréquence croissantes des cyber-attaques et des violations de données dans le monde entier, la demande d'assurance spécialisée dans les cyber-risques augmente. En effet, les assureurs constatent une demande croissante de produits de cyber-assurance couvrant les pertes liées aux attaques contre l'entreprise et la perte d'informations personnellement identifiables. Actuellement, la grande majorité de cette couverture est offerte aux États-Unis, mais la couverture s'étend géographiquement. La couverture typique comprend à la fois les pertes directes associées au coût de l'interruption d'activité (alors que les systèmes sont mis hors ligne) et les coûts indirects (tels que la compensation versée aux clients de l'assuré et les coûts d'enquête). Les polices peuvent également inclure la garantie d'une assistance pour aider à gérer l'incident.

Jusqu'à présent, les pertes cybernétiques couvertes par de contrats d'assurance ne s'élèvent qu'à environ 5 milliards de dollars, alors que le coût économique annuel de la cybercriminalité est estimé à plus de 700 milliards de dollars. En comparaison, les pertes économiques totales dues aux catastrophes naturelles et d'origine humaine en 2019 s'élevaient à environ 140 milliards de dollars, dont 56 milliards de dollars assurés, selon Swiss Re. Ces chiffres montrent le potentiel inexploité du marché de la cyber-assurance, activité qui constituera dans la décennie à venir l'un des principaux moteurs de croissance pour les assureurs des marchés développés, où certaines branches traditionnelles sont largement saturées.

Cela dit, le décollage effectif du marché dépendra de la manière dont les assureurs relèveront les défis qui y sont associés. Le risque principal est celui d'accumulation : alors qu'une catastrophe naturelle grave est limitée à une certaine région, les cyber-risques peuvent facilement se propager à travers le monde en quelques secondes, exposant un assureur à des pertes financières extrêmement élevées. Un autre défi concerne les cyber-risques silencieux, qui ne sont ni inclus ni exclus explicitement dans les polices d'assurance, ce qui peut entraîner des litiges et des réclamations imprévues encore mal pris en compte dans la tarification.

La cyber-assurance doit offrir plus qu'une simple compensation pour une perte financière potentiellement importante. Les assureurs peuvent apporter une valeur ajoutée en fournissant des services d'assistance et en aidant les assurés à mieux gérer les cyber-risques, tout en orchestrant la mise en place d'un écosystème d'expertise interne et externe pour prévenir et enquêter sur toute attaque possible. De cette manière, ils joueront alors un rôle important dans l'amélioration de la cyber-résistance.

Le type de couverture offert par La Cyber-assurance englobe un certain nombre de modules différents qui couvrent le système informatique, les données et autres activités multimédias. Ces couvertures sont normalement conçues pour inclure les éléments suivants sous une forme ou une autre :

La confidentialité des données

- Responsabilité civile
- Responsabilité suite à la divulgation d'informations commerciales et / ou personnelles confidentielles (vie privée)
- Responsabilité pour préjudice économique subi par autrui en raison d'une défaillance de la sécurité du réseau

Infractions au règlement, amendes et pénalités

• Défense d'une action réglementaire en raison d'une violation de la réglementation sur la confidentialité

• Couverture des amendes et pénalités en cas de non-respect de la réglementation en matière de confidentialité

Interruption d'activité du réseau

• Perte de revenus et dépenses engagées pendant la période d'interruption suite à une panne du système informatique ou violation de la sécurité du réseau. Les extensions peuvent couvrir les interruptions d'activité causées par la panne d'un fournisseur de services, lorsqu'elles sont causées par une panne informatique ou sécurité du réseau.

Dommages aux données et cyber-extorsion

• Destruction, corruption ou vol d'actifs d'informations électroniques et/ou de données en raison d'une panne de l'ordinateur système ou réseau.

• Menaces ou extorsions liées à la divulgation d'informations confidentielles ou à une violation de la sécurité informatique

• Un certain nombre de coûts associés à la gestion des conséquences d'une violation de la vie privée, y compris, mais sans s'y limiter à : enquête médico-légale, frais juridiques, frais de notification, frais de centre d'appels, frais de surveillance du crédit (où une pièce d'identité est volée et une marge de crédit est obtenue) et les frais de relations publiques.

Cependant, les entreprises ne sont pas certaines du niveau de couverture à acquérir et si leurs polices actuelles assurent leur protection. L'une des causes de l'incertitude tient à la difficulté de quantifier les pertes potentielles en raison du manque de données historiques pour les actuaires et les souscripteurs pour modéliser les pertes liées à la cyber-assurance. En outre, les polices traditionnelles de responsabilité civile générale ne couvrent pas toujours les cyber-risques.

Vision d'un réassureur international sur les cyber-risques :

Selon le réassureur Munich Re le plus grand souci se pose si une cyber-attaque majeure frappe une infrastructure critique comme l'électricité ou l'internet. Dans ce cas que pouvons-nous faire face à une semaine de travail sans Internet ? Ou maintenir une ligne de production sans électricité ? La plupart des entreprises ne pourraient pas poursuivre leurs activités quotidiennes et subiraient des pertes importantes.

Ces menaces ont créé à la fois un besoin de nouveaux types de couverture de cyber-assurance et un risque accru de pertes extrêmes pour les assureurs.

Dans tout le secteur de l'assurance, il est courant de faire référence au risque de défaillance des infrastructures critiques et de l'exclure des polices d'assurance cybernétique. Les experts de Munich Re, définissent les infrastructures critiques comme suit :

• Les services communs sur lesquels s'appuient toutes les entreprises ou le grand public, tels que l'électricité, les télécommunications ou Internet, lorsque ces services ne sont pas sous le contrôle, l'exploitation ou la propriété de l'assuré en question.

• Les composants physiques et les services sous-jacents nécessaires au fonctionnement de ces réseaux, tels que, dans le cas d'Internet, les fournisseurs d'accès Internet et le système de noms de domaine « DNS ».

• L'échec de ces services fait référence aux périodes où le réseau est totalement ou partiellement indisponible, globalement ou régionalement, en raison d'un évènement involontaire et non planifié affectant un grand nombre de clients.

La durée de la panne doit être suffisamment longue pour avoir un impact sur les opérations d'une entreprise, ce qui entraîne une perte de revenus ou crée une responsabilité pour le contrôleur, l'opérateur ou le propriétaire du réseau. Certaines pannes peuvent également entraîner une perte de revenus ou la création d'une responsabilité pour les clients du responsable du traitement, de l'exploitant ou du propriétaire du réseau.

Une panne d'électricité involontaire ou une panne d'Internet (y compris les services basés sur Internet) comporte un risque d'accumulation systémique, car elle aurait un impact sur un grand nombre de clients qui pourraient être exposés à des pertes significatives d'interruption d'activité. En raison de l'incertitude entourant un tel événement, il n'existe actuellement aucun moyen adéquat de modéliser la défaillance d'une infrastructure en termes quantitatifs. Et même avec des approches de modélisation en constante évolution, les assureurs seront toujours confrontés à des risques considérés comme non assurables en raison du potentiel d'accumulation sous-jacent. Cela devient plus clair lorsque l'on examine les scénarios suivants :

Scénario 1 : Panne d'électricité

L'électricité est une exigence fondamentale pour le fonctionnement des sociétés et des économies industrialisées. Les «baisses de tension» et les « coupures de courant » (panne totale de l'alimentation électrique) sont des risques à prendre en compte. Une panne de courant ou une panne de quelques minutes ne peut causer que des inconvénients mineurs, mais une panne de quelques heures, voire plusieurs jours, aurait un impact significatif sur notre vie quotidienne et sur l'ensemble de l'économie.

La préoccupation majeure est l'impact potentiel sur les infrastructures critiques : communication et transport, chauffage et approvisionnement en eau, processus de production et commerce, services d'urgence (pompiers, police, hôpitaux, commerce financier, distributeurs automatiques de billets et supermarchés…). En fin de compte, cela conduirait à un scénario catastrophique, y compris des troubles civils.

Les déclencheurs possibles d'une panne d'électricité comprennent les dangers bien connus (catastrophes naturelles, erreurs humaines et attaques terroristes / guerrières) allant au phénomène plus récent des cyber-attaques. Différentes vulnérabilités peuvent être exploitées pour provoquer des déséquilibres dans un réseau électrique, comme des pirates informatiques infiltrant les systèmes de contrôle ou la manipulation de transformateurs ou de générateurs.

Les conséquences peuvent inclure la destruction physique des pièces critiques du réseau (générateurs, transformateurs…). Si une destruction physique se produit, cela déclencherait directement une interruption d'activité assurée ou des pertes éventuelles d'interruption d'activité, lorsqu'il existe des extensions pour les fournisseurs critiques dans les polices des biens concernés. Une telle panne causée par une cyber-attaque présente un potentiel d'accumulation important de cyber-pertes.

Pourtant, il existe un potentiel d'accumulation encore plus grand pour les pertes commerciales et les pertes d'exploitation éventuelles généralement couvertes dans les polices de cyber-assurance. Pendant une panne de longue durée, à moins qu'une entreprise ne dispose d'une génération de secours qui ne repose pas sur le réseau externe affecté, il y aurait probablement une interruption de travail importante, voire totale. On peut s'attendre à ce que la plupart des entreprises de la zone géographique touchée subissent une interruption de leurs activités commerciales et subissent des pertes substantielles.

En fonction de la gravité de l'attaque, la panne peut durer plusieurs jours, voire plusieurs semaines, ce qui dépasserait sans aucun doute les périodes d'attente (ou «franchises temporelles») convenues dans les couvertures pour interruption d'activité ou interruption d'activité contingente.

Ce scénario peut conduire à des pertes étendues et généralisées sans provision pour dommages physiques.

Une autre conséquence ultérieure des coupures d'électricité peut être des pannes Internet à grande échelle. Bien sûr, ceux-ci peuvent également se produire indépendamment.

Scénario 2 : défaillance de l'infrastructure Internet

Les cyber-attaques représentent une menace croissante pour les infrastructures Internet. Les attaques par déni du service distribué « DDoS » gagnent du terrain comme un exemple marquant d'une telle source de risque. Les pirates cherchent à rendre une machine ou une ressource réseau indisponible pour ses utilisateurs visés en perturbant temporairement ou indéfiniment les services d'un hôte connectée à Internet. Si l'attaque touche un serveur DNS ou un domaine, elle peut entraîner une interruption d'activité généralisée, en particulier dans le secteur du commerce électronique.

En outre, tous les autres segments d'activité qui utilisent Internet peuvent subir une interruption d'activité sans aucune perte physique ni dommage aux données, simplement parce que le DNS ne peut pas faire face au nombre extrêmement élevé de demandes.

Quels scénarios sont et ne sont pas considérés comme assurables ?

Selon le réassureur Munich Re, Il existe des scénarios de pannes considérés comme assurables. Cela comprend la défaillance des systèmes informatiques sous le contrôle de l'assuré, ainsi que des éléments supplémentaires sous leur contrôle direct, tels que les générateurs de secours. Dans ces cas, le potentiel d'accumulation des dépendances à des infrastructures externes peut être évité.

En outre, les pannes d'entités tierces (par exemple les fournisseurs de services informatiques) peuvent être couvertes, à l'exception de l'infrastructure considérée comme essentielle pour des réseaux comme Internet.

Les approches de modélisation utilisées par les assureurs pour quantifier le cyber-risque s'améliorent continuellement. Cependant, certaines sources de cyber-risque sont considérées comme non assurables en raison du potentiel d'accumulation sous-jacent, comme dans les deux scénarios décrits ci-dessus. L'exposition à l'accumulation est la défaillance d'infrastructure affectant un grand nombre de clients, avec une exposition énorme aux pertes d'exploitation.

Exemples de Cyber-attaques

Le plus gros problème auquel sont confrontés les entreprises et les utilisateurs est l'incapacité d'accéder à leurs systèmes et données, ce qui provoque une perturbation de la productivité. Les attaques de ransomwares sont considérées comme l'une des menaces les plus rapides à croitre de la cybercriminalité. En effet, les incidents y relatifs se multiplient à un rythme alarmant.

On peut énumérer différents types de Cyber-attaques selon leur nature et objectifs :

- **Attaques aveugles**

Ces attaques sont de grande envergure mondiale et ne semblent pas faire de discrimination entre les gouvernements et les entreprises:

- **Attaque du ransomware** WannaCry le 12 mai 2017 affectant des centaines de milliers d'ordinateurs dans plus de 150 pays:

Une attaque de ransomware connue sous le nom de «WannaCry» a touché plus de 200 000 ordinateurs dans le monde. Particuliers, entreprises et organisations dans plus de 150 pays auraient été touchés.

L'attaque « WannaCry » a exploité une vulnérabilité connue dans les anciennes versions de Microsoft Windows. Bien que Microsoft eût publié un correctif pour cela après que la vulnérabilité avait été identifiée, le logiciel malveillant a pu être téléchargé sur des ordinateurs via des liens dans e-mails. « WannaCry » semble également avoir la capacité se répandre entre des ordinateurs qui ont la même vulnérabilité.

Entreprises et utilisateurs des ordinateurs concernés ont été confrontés à une demande de rançon en bitcoin pour restaurer leurs systèmes. Le plus grand impact semble avoir été sur les services des prestations sanitaires.

- **Attaques destructives**

Ces attaques sont liées au fait d'infliger des dommages à des organisations spécifiques :

- Opération Ababil, menée contre des institutions financières américaines

- Cyberattaque TV5 Monde d'avril 2015.

- Shamoon, un virus informatique modulaire, a été utilisé en 2012 dans une attaque contre 30 000 postes de travail de la compagnie Saoudinne Aramco, obligeant l'entreprise à passer une semaine à restaurer ses services.

• Cyber-guerre

Il s'agit d'attaques destructrices à motivation politique visant au sabotage et à l'espionnage.

- En 2007, le groupe de hackers APT28 (Advanced Persistant Menace 28), également appelée « Fancy Bear », fait sa première apparition publique. Ils se spécialisent dans des institutions de premier plan et apparaissent principalement dans des contextes politiques. Au début, des experts ont rencontré plusieurs programmes malveillants, certains développés par le groupe lui-même. Pendant le conflit du Caucase, plusieurs ministères géorgiens ont été piraté par le groupe. Mais ce n'était que le début : en 2014/15, Fancy Bear a systématiquement infiltré les Ministères de la défense de plusieurs États européens : Bulgarie, Pologne, Hongrie, Albanie et Danemark.

En 2015, Fancy Bear a infiltré les systèmes informatiques de le Bundestag allemand. Les bureaux d'au moins 16 des parlementaires ont été passés au peigne fin, les boîtes aux lettres copiées, disques durs scrutés et une bonne partie des données internes est probablement classée détournée.

Un an plus tard, l'infiltration et la violation de données du Parti démocrate américain lors de la campagne électorale d'Hillary Clinton ont été attribués à l'APT28 par le FBI. Leur dernière apparition remonte à 2017, lorsque le siège de la campagne présidentielle française du candidat Emmanuel Macron a été piraté.

- Vestige est également soupçonné d'être à l'origine d'une attaque de harponnage en août 2016 contre des membres du Bundestag et de multiples partis. Les autorités craignent que des informations sensibles puissent être recueillies par des pirates informatiques pour manipuler plus tard le public avant des élections telles que les élections fédérales allemandes de 2017.

• Espionnage gouvernemental

Ces attaques concernent le vol d'informations auprès d'organisations gouvernementales.

- Cyberattaque de 2008 contre les États-Unis, cyber-espionnage visant les ordinateurs militaires américains.

- Cyber-attaque lors du sommet du G20 à Paris, ciblant des documents liés au G20, y compris des informations financières

- Google - en 2009, les pirates ont violé les serveurs d'entreprise de Google et ont eu accès à une base de données contenant des informations classifiées sur des espions, des agents et des terroristes présumés sous la surveillance du gouvernement américain.

• L'espionnage industriel

Ces attaques concernent le vol de données d'entreprises liées à des méthodes de production ou à des produits ou endommager les machines et process de production.

- En 2015, la production dans une biscuiterie canadienne s'est arrêtée après que des pirates ont infiltré son réseau.

  Les cybercriminels ont utilisé un logiciel pour analyser le réseau de l'usine et ont pris le contrôle de ses Systèmes PLC (automates programmables).

  La production était arrêtée et le mélange de biscuits qui avait déjà été produit a séché dans les tubes de transport.

  Les blocages causés par le mélange étaient si mauvais que les tuyaux ont dû être démontés et remplacé, entraînant une grave interruption des activités pour le fabricant.

- Un grand constructeur automobile et sa société partenaire ont trouvé des écrans d'ordinateur dans plusieurs usines intelligentes afficher l'image redoutée de Bitcoin et la rançon demandée. Les dégâts ont commencé lorsque le «WannaCry» a verrouillé les fichiers cryptés et bloqué l'accès au PC dans une installation ce qui a arrêté toute l'activité et a arrêté la production de travail de 3 500 salariés.

  Puisque le virus peut se propager à travers des réseaux interconnectés, deux usines tout au long de la chaîne de production ainsi qu'une société partenaire ont été contraintes de cesser la production.

  Les pertes des entreprises pour rester hors ligne, payer les travailleurs inactifs pendant plusieurs jours et les restaurations informatiques dépassaient de loin la demande de rançon demandée. Avec un arrêt coûtant des millions de dollars par jour, la prévention des risques de sécurité informatique probables aurait été inestimables.

- En 2014, une aciérie allemande a été la cible d'une cyber-attaque. Des hackers ont pris le contrôle du logiciel de production causant des dommages matériels importants au site.

  Les attaquants ont d'abord piraté le logiciel bureautique du site réseau en envoyant des e-mails de phishing et infiltré le système avec des logiciels malveillants. Ils ont ensuite piraté le logiciel de gestion de la production, reprenant la plupart des systèmes de contrôle de l'usine. Ils ont réussi à empêcher un haut fourneau d'initier ses mesures de sécurité à temps, causant de graves dommages à l'infrastructure.

  La motivation des hackers n'est toujours pas claire. Toutefois, cette attaque a été classée comme une attaque avancée.

• Adresses e-mail et identifiants de connexion volés

Ces attaques concernent le vol d'informations de connexion pour des ressources Web spécifiques.

- eBay : eBay a signalé qu'une attaque a révélé la liste complète de ses comptes de 145 millions d'utilisateurs en mai 2014, y compris les noms, adresses, dates de naissance et mots de passe cryptés. Le géant des enchères en ligne a déclaré que les pirates utilisaient les informations d'identification de trois employés de l'entreprise pour accéder à son réseau et avaient un accès complet pendant 229 jours - plus que suffisamment de temps pour compromettre la base de données des utilisateurs.

L'entreprise a demandé aux clients de changer leurs mots de passe. Les informations financières, telles que les numéros de carte de crédit, ont été stockées séparément et n'ont pas été compromises. L'entreprise a été critiquée à l'époque pour un manque de communication avec ses utilisateurs et une mauvaise mise en œuvre du processus de renouvellement des mots de passe.

- Adobe : en 2013, des pirates informatiques ont obtenu l'accès aux réseaux d'Adobe, volé des informations sur les utilisateurs et téléchargé le code source de certains programmes Adobe. Il a attaqué 150 millions de clients.

Un accord conclu en août 2015 demandait à Adobe de verser 1,1 million de dollars en frais juridiques et un montant non divulgué aux utilisateurs pour régler les réclamations pour violation de la loi sur les dossiers clients et pratiques commerciales déloyales. En novembre 2016, le montant payé aux clients était de 1 million de dollars.

- Yahoo! : en 2012, les pirates ont publié des informations de connexion pour plus de 453 000 comptes d'utilisateurs. De nouveau en janvier 2013 et en janvier 2014.

Yahoo a annoncé en septembre 2016 qu'il avait été victime en 2014 de ce qui serait la plus grande violation de données de l'histoire.

Puis, en décembre 2016, Yahoo a révélé une autre faille de 2013 par un autre attaquant qui avait compromis les noms, les dates de naissance, les adresses e-mail et les mots de passe, ainsi que les questions et réponses de sécurité d'un milliard de comptes d'utilisateurs. Yahoo a révisé cette estimation en octobre 2017 pour inclure l'ensemble de ses 3 milliards de comptes d'utilisateurs.

Le timing de l'annonce initiale de la violation était mauvais, car Yahoo était en cours d'acquisition par Verizon, qui a finalement payé 4,48 milliards de dollars pour l'activité Internet de base de Yahoo. Les violations ont fait perdre environ 350 millions de dollars à la valeur de l'entreprise.

- En 2015, un important site de rencontre en ligne pour mariage a été piraté par un groupe qui s'est identifié comme « The Impact Team ». Les pirates ont menacé de divulguer les informations personnelles des utilisateurs si le site n'était pas mis hors ligne. Les opérateurs de l'entreprise basée à Toronto ont annoncé avoir supprimé des informations de leur site qui pourrait être utilisées pour identifier les utilisateurs mais, peu de temps après, exactement ces informations sensibles ont été divulguées en ligne.

Les noms, adresses postales et e-mail, téléphone Nombres, sexe, dates de naissance, légendes de profil, poids, statuts relationnels, préférences sexuelles, informations de carte de crédit et historique des transactions de 30 à 40 millions d'utilisateurs du service de rencontres ont été publiés.

En conséquence, l'entreprise a perdu environ un quart de ses revenus annuels, des suicides ont été signalés, des démissions et des ruptures de mariage. Une enquête officielle a été ouverte dont les résultats ont été publiés dans un rapport indiquant que les mesures de sécurité l'entreprise faisaient défaut ; son utilisation d'un une fausse vérification de sécurité était trompeuse.

Peu de temps après, un recours collectif national a été lancé contre les propriétaires et les exploitants. Ce procès était déposé au nom de tous les résidents canadiens abonnés sur le site Web. Le demandeur a réclamé 760 millions de dollars américains en dommages.

- **Carte de crédit et données financières volées**

  - Faille de données Equifax 2017

    En 2017, Equifax, l'un des plus grands bureaux de crédit aux États-Unis, a annoncé qu'une faille de cybersécurité s'est produite entre mai et la mi-juillet de cette année. Les cybercriminels avaient accédé à environ 145,5 millions de données personnelles des consommateurs américains d'Equifax, y compris leurs noms complets, numéros de sécurité sociale, informations de carte de crédit, dates de naissance, adresses et, dans certains cas, numéros de permis de conduire.

    - Violation de données des banques indiennes en 2016 - On estime que 3,2 millions de cartes de débit ont été compromises. Les principales banques indiennes - SBI, HDFC Bank, ICICI, YES Bank et Axis Bank ont été parmi les plus touchées.

    - En février 2016, des hackers avaient tenté de voler un milliard de dollars de la banque centrale du Bangladesh en manipulant les Transactions SWIFT. Il semble que les auteurs ont piraté des ordinateurs avec lesquels des messages SWIFT sont envoyés et des transferts demandés de grandes sommes du compte de la Banque du Bangladesh auprès de la Réserve fédérale de New York. Bien que la plupart des transferts ont été bloqués, les pirates ont capturé 81 millions de dollars américains transférés aux casinos et aux agents de casino aux Philippines.

    Au moins 15 millions de dollars des fonds volés ont été récupérés avec l'aide du conseil Anti Blanchiment d'argent Philippin (Philippines Anti-Money Laundering Council).

Selon les enquêteurs, la banque centrale du Bengladesh n'avait pas protégé ses ordinateurs avec un pare-feu et avait utilisé des systèmes matériels non sécurisés.

- Target Corporation :

L'un des plus grands détaillants aux États-Unis, Target Corporation, a subi une cyber-violation massive à la fin de 2013. Un intrus a accédé et a volé des données de carte de paiement sur environ 40 millions de comptes de cartes de crédit et de débit de clients ayant effectué des achats dans ses magasins aux États-Unis entre le 27 novembre et le 17 décembre 2013 via un logiciel malveillant installé sur son système de point de vente dans les magasins américains de Target. De plus, l'intrus a volé certaines informations sur les clients, notamment noms, adresses postales, numéros de téléphone ou adresses e-mail, pour jusqu'à 70 millions de personnes. La résultante, la publicité de l'événement a coûté à l'entreprise un montant important en ventes perdues, en perte de réputation, en recours collectifs et l'éviction de son directeur général.

Depuis la violation de données, Target a engagé 88 millions USD de dépenses cumulées, partiellement compensées par les des recouvrements d'assurance de 52 millions USD, pour des dépenses cumulées nettes de 35 millions USD. Pour limiter son exposition aux pertes liées à la violation de données et autres réclamations, le détaillant déclare qu'il maintient une couverture d'assurance de sécurité du réseau de 100 millions USD, au-dessus de 10 millions USD déductible. Cette couverture et certaines autres couvertures d'assurance commerciale habituelles réduisent l'exposition de Target à la violation de données, a expliqué l'entreprise dans son dépôt.

- VISA et MasterCard - en 2012, ils ont averti les banques émettrices de cartes qu'un processeur de paiement tiers avait subi une faille de sécurité, affectant jusqu'à 10 millions de cartes de crédit.

- MasterCard - en 2005, la société a annoncé que jusqu'à 40 millions de titulaires de carte auraient pu se faire voler des informations de compte en raison du piratage d'un de ses processeurs de paiement.

• Données médicales volées

Au cours des dernières années, les données relatives au secteur de la santé sont devenues l'atout le plus précieux pour les pirates. Les établissements de santé n'ont jusqu'à présent pas été suffisamment protégés contre les cyberattaques. Les serveurs des cabinets médicaux et hôspitaliers hébergent les données sensibles des patients et des maladies. Les documents et sont connectés en permanence à l'Internet.

En août 2014, les systèmes de la « Health Community Systems », une association de 206 hôpitaux, ont été infiltrés et 4,5 millions de dossiers médicaux ont été volés, y compris les noms, identifiants sociaux, adresses et numéros de téléphone.

Au tournant de l'année 2015/2016, 28 hôpital allemand ont été victimes de cyberattaques. Deux des attaques étaient critiques : les pirates ont réussi à s'infiltrer aux systèmes informatiques avec un logiciel malveillant qui a crypté toutes les données. A Neuss, l'attaque était accompagnée par une tentative de chantage. Les deux hôpitaux avaient fermé complètement leurs réseaux informatiques afin d'éradiquer les virus.

À l'ère de la numérisation et de la santé numérique, les cyberattaques peuvent littéralement menacer la vie de patients du monde entier.

Cyber risk au temps du Covid

Alors que la pandémie de COVID-19 accélère significativement la transformation numérique de nombreuses organisations, le risque de cyber-attaques augmente inévitablement. En effet, le paysage des cyber-menaces de 2020 a évolué avec la pandémie du Covid 19 et la multiplication des attaques suite au recours au télétravail imposé par les mesures de confinement prises pour faire face à cette pandémie. Les pirates et les stratagèmes de phishing cherchent à tirer parti de la situation actuelle pour accéder aux données personnelles, financières et des entreprises.

• Augmentation des attaques de phishing

Les attaques de phishing sont en augmentation. Les programmes de phishing utilisent des e-mails, des textes ou d'autres outils de communications pour inciter les utilisateurs à télécharger des logiciels malveillants ou à partager des informations confidentielles. Les escroqueries par hameçonnage d'aujourd'hui s'appuient sur la peur et le besoin d'informations sur le coronavirus. Les services secrets américains ont émis un avertissement concernant une augmentation des e-mails de phishing qui semblent provenir d'organisations réputées telles que l'Organisation mondiale de la santé.

Alors que les personnes soucieuses d'informations sur la propagation du coronavirus recherchent des informations fiables, la carte de l'Université Johns Hopkins a fourni une source de détails vérifiée et digne de confiance sur les infections. Malheureusement, les experts du secteur signalent que les logiciels malveillants usurpent l'identité du site et compromettent les informations personnelles.

• De faux sites Web cherchent à compromettre les informations d'identification

Selon Trend Micro, les faux sites Web sont une autre arnaque dont les particuliers et les entreprises doivent se méfier. Dans plusieurs cas, les sites semblent avoir été créés par des agences gouvernementales et demandent des informations personnelles afin de s'inscrire sur une liste d'attente pour des vaccins, des informations ou une aide financière. Certains de ces sites encouragent les utilisateurs à se connecter en utilisant les informations d'identification de leur entreprise, ce qui pourrait mettre en danger les systèmes de l'entreprise et d'autres réseaux sécurisés.

• Outils de travail à domicile frauduleux

Les agences de cybersécurité du Royaume-Uni et des États-Unis ont averti les entreprises et les employés que des fraudeurs tentent d'inciter les utilisateurs à télécharger des logiciels malveillants ou à fournir des informations financières en échange d'outils de travail à domicile.

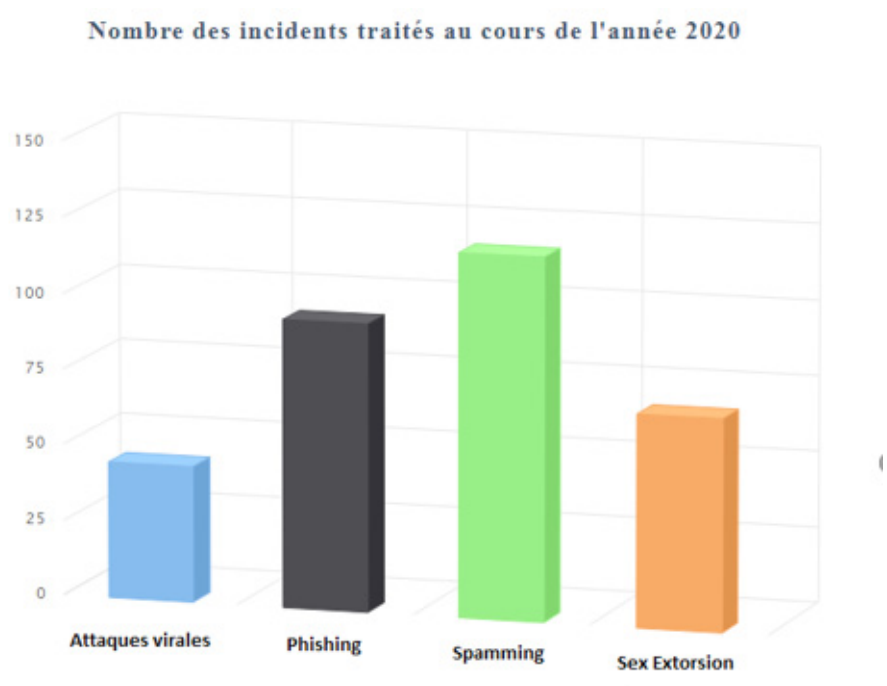
• Les escroqueries interentreprises sont en hausse

L'approvisionnement en produits et fournitures est un autre domaine dans lequel les entreprises doivent être vigilantes. Les prévisions sur la longue durée de la pandémie, qui devrait durer au moins plusieurs mois, inciteront probablement les gangs de phishing à investir dans le développement des escroqueries, comme se faire passer pour des fournisseurs médicaux et inciter les hôpitaux et les cliniques à leur acheter des produits inexistants. Comme les perturbations de la chaîne d'approvisionnement ont un impact sur d'autres industries, ces escroqueries peuvent avoir un impact sur les entreprises qui acquièrent des articles physiques ou des licences numériques.

Cyber Risque en Tunisie

Le nombre de cyberattaques a connu une augmentation de 20% durant la crise du Covid-19 en Tunisie selon les propos du ministre des technologies de la Communication en novembre 2020. Le ministre a plaidé pour la mise en place d'un mécanisme capable de faire face à ce phénomène, signalant que de grandes sociétés ont été victimes de ces cyberattaques et subissent à ce jour leurs conséquences. Il a insisté aussi que la sécurité cybernétique fait partie des priorités de son département.

De son côté, l'Agence Nationale de Sécurité Informatique (ANSI) a appelé toutes les structures et les institutions nationales à renforcer leur niveau de vigilance face au risque d'augmentation des piratages informatiques. Un groupe de pirates a profité de la situation sanitaire critique que traversent les différents pays du monde et ont mené des cyber-attaques à savoir une attaque par déni de service (DDoS).



Incident : Tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service.

Les équipes de l'Agence nationale de la sécurité informatique ont traité 330 incidents au cours de l'année 2020.

Selon l'ANSI, ces attaques ont visé les distributeurs de la Poste et les processus liés au travail à distance. D'ailleurs, plusieurs pays européens ont décidé de suspendre les services postaux électroniques.

L'ANSI appelle à prendre les mesures opérationnelles nécessaires et de permettre uniquement aux personnes ayant une identité et une adresse IP tunisienne d'accéder aux systèmes informatiques.

Par ailleurs, l'Agence nationale de la Sécurité Informatique a confirmé au mois de Février 2021 dernier qu'une importante banque tunisienne a été victime d'une importante cyberattaque, son système informatique a été piraté et des perturbations dans quelques agences du réseau commercial ont été remarquées. En effet, des pirates sont parvenus à pirater le système informatique de cette banque en dépit des grands dispositifs de sécurité informatique, ce qui a provoqué un état de paralysie dans son système.

Cette action de piratage aurait été faite par la technique de Phishing utilisée par les fraudeurs pour obtenir des renseignements personnels et d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance.

Selon un communiqué de la banque, ses équipes se sont mobilisées pour résoudre l'incident et assurer la continuité de l'ensemble des opérations dans les meilleures conditions possibles.

La banque confirme aussi que le problème rencontré n'a pas touché son système de production et que la situation est maîtrisée.

Par ailleurs, et dans un communiqué rendu public, l'ANSI met en garde contre le « Whaling », une cyberattaque qui consiste à usurper l'identité d'un haut responsable ou dirigeant au sein d'une entreprise, afin de piéger ses collaborateurs. Le but d'une telle attaque est d'avoir accès à des informations confidentielles ou même, d'inciter ces collaborateurs à effectuer des opérations financières frauduleuses.

Le « Whaling » (chasse à la baleine) ne cible pas des victimes ordinaires mais vise, essentiellement, les hauts dirigeants influents au sein d'une entreprise, en usurpant l'identité d'un haut responsable (directeur financier ou même le PDG) dans le but d'avoir accès à des informations confidentielles ou sensibles, indique l'organisme gouvernemental.

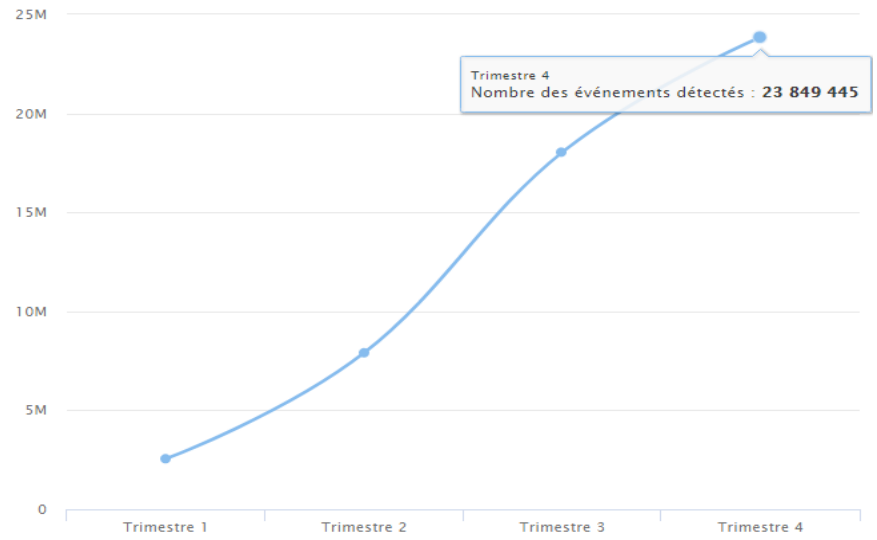
Dans un autre incident, des utilisateurs de cartes « e-dinar Travel », réservées aux allocations de voyage à l'étranger ont été victimes de piratage électronique a annoncé la Poste Tunisienne sur son portail électronique.

Selon la Poste cette opération a été interrompue à temps. La source a été identifiée et des procédures judiciaires ont été engagées contre les auteurs de cette escroquerie électronique.

De plus, la Poste Tunisienne s'est engagée avec le concours de ses partenaires internationaux, à indemniser les clients, victimes de cette opération, conformément aux dispositions en vigueur.

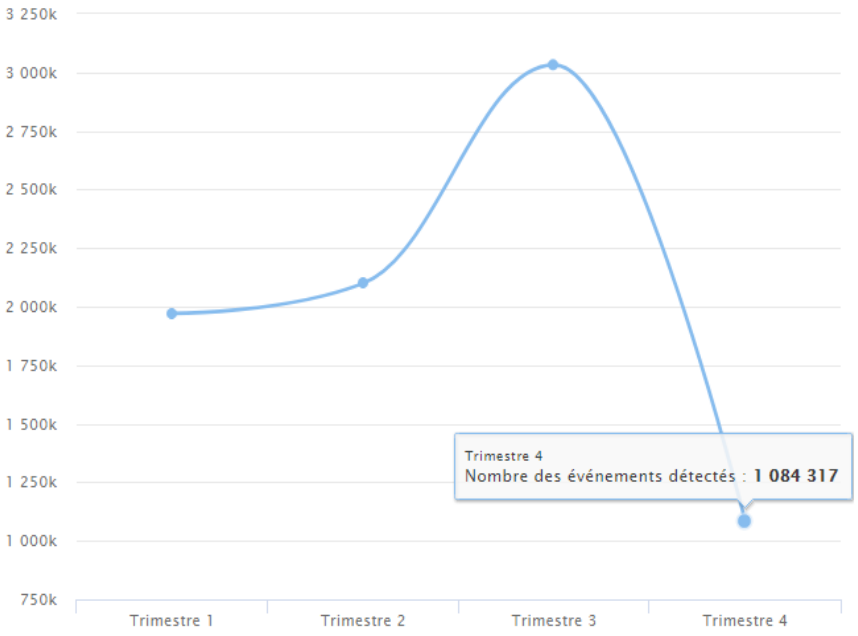
Les courbes ci-dessous de l'Agence nationale de la Sécurité Informatique, montrent l'évolution du nombre des évènements détectés pour les années 2019 et 2020. Un évènement est défini selon l'agence par l'exploitation d'une faille dans le but de réaliser une tentative d'attaque. Il en résulte que le nombre de cas est de loin plus élevé en 2020 et la courbe ascendante tout au long de l'année 2020 montre à quel point la pandémie du Covid a contribué à la multiplication des cyber-attaques, phénomène expliqué par le recours au télétravail et aux outils de travail à distance et à l'utilisation accrue de l'internet pour s'informer sur cette pandémie et les mesures à suivre pour y faire face.

Evolution du nombre des événements détectés au cours de l'année 2020



Un **événement** est l'exploitation d'une faille dans le but de réaliser une tentative d'attaque.

Évolution du nombre des événements détectés au cours de l'année 2019



Risques Emergents

4. L’interruption d’activité sans dommages

Le risque d'interruption d'activité est simplement «tout ce qui interrompt l'activité ».

L'assurance pertes d'exploitation, permet aux entreprises de compenser les effets de la diminution du chiffre d'affaires et de faire face à une interruption d'activité souvent longue, voire à un arrêt total de sa production entraînant des conséquences financières importantes. Cette assurance couvre les charges fixes et permanentes (amortissements, impôts et taxes, loyers, rémunération du personnel, intérêts d'emprunt…). Cette garantie est strictement corrélée à la survenance d'un sinistre couvert causant des dommages matériels direct tels que l'incendie, explosion, acte de terrorisme, dégâts des eaux, bris de machine, ….

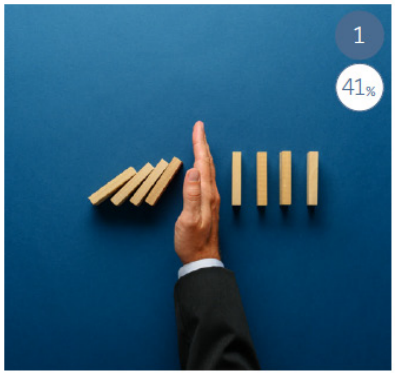
En 2010, suite à l'éruption du volcan islandais Eyjafjallajökull qui a dégagé d'énormes nuages de cendres et de roches, le trafic aérien a été paralysé pendant plusieurs jours à l'échelle mondiale, les avions cloués au sol et toute une partie de l'Europe du nord était recouverte de cendres. Les pertes étaient importantes pour les compagnies aériennes et les professionnels du tourisme. Toutefois, ces entreprises étaient privées de tout recours sur le terrain de l'assurance puisque l'assurance PE ne peut jouer qu'après l'arrêt ou la diminution d'activité à la suite d'un «événement garanti». C'est ainsi qu'il a fallu repenser la couverture de pertes d'exploitation sans dommage.

Aujourd'hui, les nouveaux déclencheurs d'interruption d'activité sans dommage peuvent aller des Eruptions volcaniques avec propagation de cendres à la Cybercriminalité, Menaces terroristes, conditions climatiques exceptionnelles, évolution du paysage politique, embargo à l'autre bout de la planète , voire même la propagation d'une pandémie qui met tout le globe en confinement. Ce qui rend essentiel pour les risk managers de comprendre les menaces en constante évolution auxquelles les entreprises sont confrontées.

Selon le Baromètre des risques Allianz 2021, l'interruption d'activité demeure le principal risque auquel les entreprises sont confrontées pour la huitième année consécutive. Cependant, parallèlement aux risques physiques d'incendie, d'explosion et de catastrophes naturelles, les causes non dommageables de l'interruption des activités émergent constamment et deviennent un problème beaucoup plus important, entraînant potentiellement de lourdes pertes pour les entreprises sans causer de dommages matériels.

Ranking changes are determined by positions year-on-year, ahead of percentages

Rank		Percent	2020 rank	Trend
1	**Business interruption (incl. supply chain disruption)**	**41%**	2 (37%)	▲
2	Pandemic outbreak (e.g. health and workforce issues, restrictions on movement)[1]	**40%**	17 (3%)	▲
3	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	**40%**	1 (39%)	▼
4	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)[2]	**19%**	5 (21%)	▲
5	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**19%**	3 (27%)	▼
6	Natural catastrophes (e.g. storm, flood, earthquake, wildfire)	**17%**	4 (21%)	▼
7	Fire, explosion	**16%**	6 (20%)	▼
8	Macroeconomic developments (e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)[3]	**13%**	10 (11%)	▲
9	Climate change/increasing volatility of weather	**13%**	7 (17%)	▼
10	Political risks and violence (e.g. political instability, war, terrorism, civil commotion, riots and looting)	**11%**	11 (9%)	▲
11	New technologies (e.g. impact of artificial intelligence, autonomous vehicles, 3D printing, Internet of Things, nanotechnology, blockchain)[4]	**9%**	9 (13%)	▼
12	Loss of reputation or brand value (e.g. public criticism)	**9%**	8 (15%)	▼



En 2014, il a été signalé que des attaquants avaient pénétré le logiciel de gestion de la production d'une aciérie allemande et pris le contrôle de l'usine. Ils ont méthodiquement détruit les composants d'interaction homme-machine et ont réussi à empêcher un haut fourneau d'initier ses paramètres de sécurité, causant de graves dommages matériels à l'infrastructure et par conséquence une interruption totale de l'activité de l'usine.

C'est un exemple type de sinistre PE sans dommages.

TOP RISKS BY COMPANY SIZE

TOP 10 RISKS FOR LARGE-SIZE COMPANIES*

*>US$500mn annual revenues

Source: Allianz Global Corporate & Specialty.

Figures represent how often a risk was selected as a percentage of all responses for that company size.

Respondents: 1,234

Figures don't add up to 100% as up to three risks could be selected.

1 Business interruption ranks higher than cyber incidents based on the actual number of responses

2 Changes in legislation and regulation ranks higher than market developments based on the actual number of responses

Rank		Percent	2020 rank	Trend
1	Business interruption (incl. supply chain disruption)[1]	46%	1 (43%)	=
2	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	46%	2 (43%)	=
3	Pandemic outbreak (e.g. health and workforce issues, restrictions on movement)	38%	NEW	▲
4	Natural catastrophes (e.g. storm, flood, earthquake, wildfire)	19%	4 (23%)	=
5	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)[2]	18%	3 (27%)	▼
6	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	18%	7 (18%)	▲
7	Fire, explosion	16%	5 (20%)	▼
8	Climate change/increasing volatility of weather	15%	6 (18%)	▼
9	Macroeconomic developments (e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)	12%	10 (10%)	▲
10	Political risks and violence (e.g. political instability, war, terrorism, civil commotion, riots and looting)	11%	NEW	▲

TOP 10 RISKS FOR MID-SIZE COMPANIES*

*$250mn to $500mn annual revenues

Source: Allianz Global Corporate & Specialty.

Figures represent how often a risk was selected as a percentage of all responses for that company size.

Respondents: 495

Figures don't add up to 100% as up to three risks could be selected.

1 Fire, explosion ranks higher than market developments based on the actual number of responses

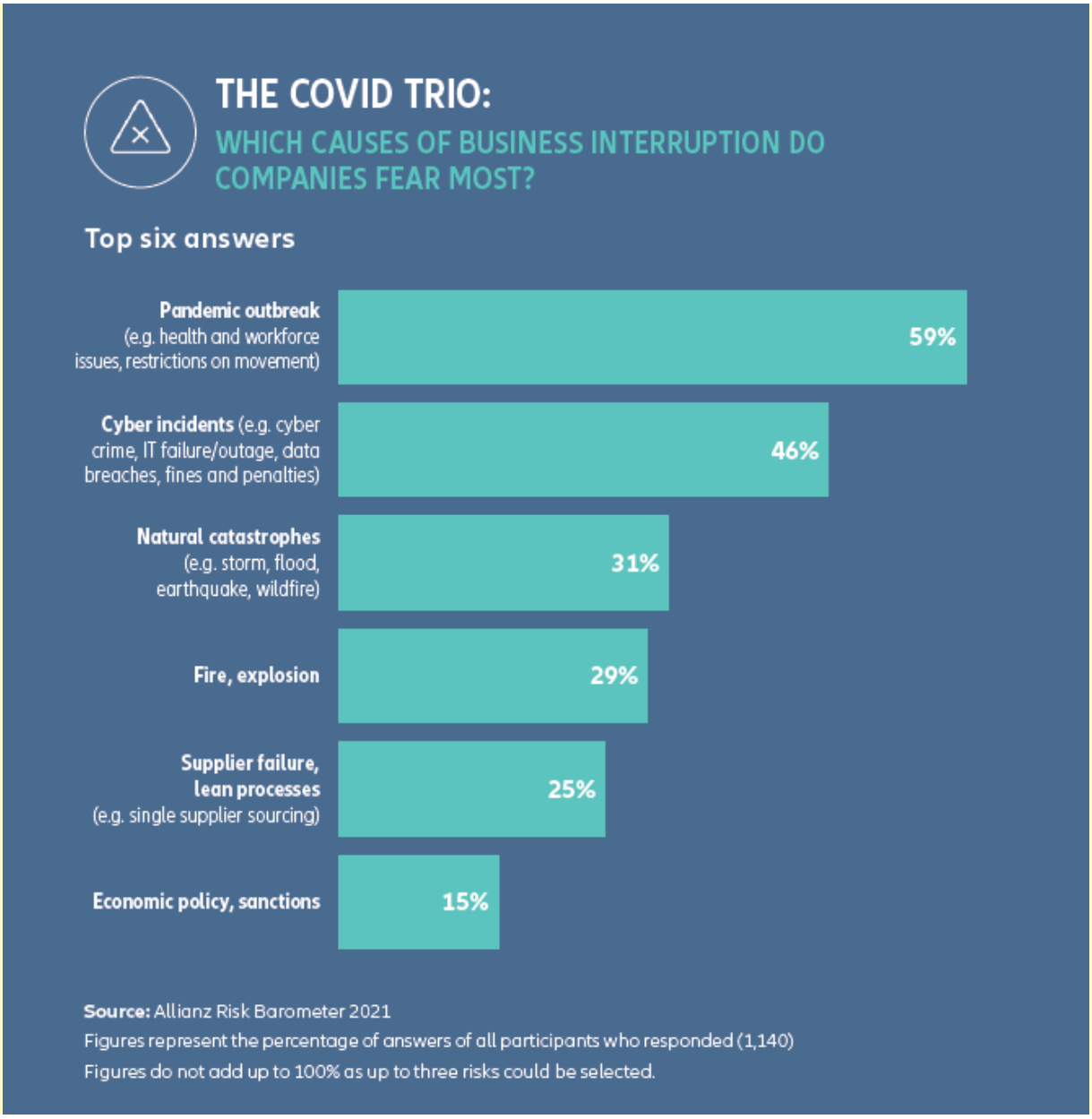
Rank		Percent	2020 rank	Trend
1	Business interruption (incl. supply chain disruption)	44%	1 (37%)	=
2	Pandemic outbreak (e.g. health and workforce issues, restrictions on movement)	40%	NEW	▲
3	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	34%	2 (36%)	▼
4	Natural catastrophes (e.g. storm, flood, earthquake, wildfire)	21%	5 (19%)	▲
5	Fire, explosion[1]	20%	4 (22%)	▼
6	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	20%	6 (19%)	=
7	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	16%	3 (25%)	▼
8	Climate change/increasing volatility of weather	13%	7 (17%)	▼
9	Macroeconomic developments (e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)	12%	10 (10%)	▲
10	Political risks and violence (e.g. political instability, war, terrorism, civil commotion, riots and looting)	11%	NEW	▲

Un risque complexe et difficile à modéliser

Malgré que les chefs d'entreprises du monde entier sont attentifs au risque d'interruption d'activité et que la résilience est intégrée dans la plupart des entreprises dans la mesure du possible, des chaînes d'approvisionnement complexes, souvent internationales et interdépendantes peuvent rapidement s'arrêter si un lien se rompt, et peu d'entreprises sont entièrement en mesure d'éviter une certaine forme d'interruption d'activité. Et aucune préparation avancée ne permettra à une entreprise d'évaluer le transfert des risques pour déterminer quel niveau de couverture d'assurance est approprié et abordable et quel soutien est disponible en cas d'interruption d'activité.

Pour les assureurs, le risque PE peut être physique, virtuel, réputationnel et surtout financier. C'est ce qui en fait l'un des domaines d'assurance les plus mal compris et de nombreux professionnels du risque sont mal préparés aux complexités qui accompagnent une interruption d'activité, d'autant plus quand il s'agit de PE sans dommage. Bref, l'assurance ne sait pas encore correctement appréhender la perte d'exploitation sans dommages.

D'ailleurs, les assureurs rencontrent des difficultés pour établir avec précision la couverture et, plus ardu encore, traiter un sinistre peut tester même le gestionnaire le plus expérimenté.



Dans l'environnement actuel de l'assurance, les souscripteurs PE s'intéressent plus à la capacité d'une entreprise à répondre à un événement et un certain nombre d'assureurs émettent de fortes recommandations pour que des plans d'intervention soient élaborés et testés. Lorsqu'aucun plan de continuité des activités ou de gestion de crise n'existe, cela pourrait avoir un impact sur la tarification ou la volonté de l'assureur de couvrir le risque. La planification de la continuité des activités doit devenir plus holistique et dynamique. Les plans doivent être constamment mis à jour et testés, y compris avoir des fournisseurs alternatifs disponibles.

C'est en fait de l'assurance sur-mesure, d'autant que les garanties sont accordées sur la base de « périls dénommés », c'est-à-dire de certains facteurs déclencheurs. Certes, le marché se développe mais reste extrêmement contrasté avec des assureurs qui ont cherché à bâtir des couvertures dédiées, d'autres qui ont étendu leur couverture à quelques garanties en premier risque et ceux qui ont simplement choisi la solution du fronting.

Zurich et Allianz par exemple, proposent de couvrir la carence de la chaîne logistique avec comme déclencheur un péril tel que l'insolvabilité du client et non plus un dommage. Par contre Munich Re a choisi de se concentrer sur les besoins des grandes entreprises en proposant une couverture PE consécutive à l'arrêt d'un site en raison de la décision d'une autorité avec une capacité allant jusqu'à 150 M €. Et Beazley couvre les PE suite à une attaque terroriste dont l'assuré n'a pas été directement la cible.

La tendance émergente est aussi que les risk-managers prennent le contrôle de leurs propres données sur les risques, en commençant par des enquêtes, et prennent le contrôle des négociations d'assurance. Avec leurs propres données, enquêtes, informations sur l'exposition à l'interruption d'activité et résultats de la modélisation des catastrophes naturelles, les risk managers peuvent comparer le niveau de protection et le rapport qualité-prix d'assurance et établir eux-mêmes la position optimale en ce qui concerne la couverture, la tarification, les franchises et les limites.

Ceci confirme les complexités qui accompagnent une perte d'exploitation typique. Il faut de 12 à 18 mois ou plus pour documenter, négocier et régler complètement un sinistre PE important et complexe selon la taille et les circonstances entourant l'événement ayant entraîné la perte. Qu'en est-il pour les sinistres de PE sans dommage ? Les sinistres pour interruption d'activité sans dommage sont rarement simples et donnent généralement lieu à une série de négociations entre l'assuré et les assureurs, même avec les professionnels du risque qui ont déjà vécu des pertes dans le passé.

Indépendamment du fait qu'elle résulte d'expositions traditionnelles telles qu'un incendie dans une usine de fabrication ou une catastrophe naturelle qui a un impact sur la production, une rupture de la chaîne d'approvisionnement due à des dommages matériels dans les locaux d'un fournisseur ou d'un client (souvent appelée PE contingente CPE) ou encore une émeute ou des troubles civils, la PE peut avoir un effet considérable sur les revenus d'une entreprise, même si l'événement se produisait à des milliers de kilomètres. Et son impact peut être l'un des risques les plus difficiles à mesurer et à modéliser.

Pour relever le défi du risque d'interruption d'activité, les assureurs et risk-managers doivent trouver des moyens de quantifier les expositions.

Les Perturbations de la chaîne d'approvisionnement

Il s'agit d'une forme d'interruption d'activité dont les dégâts sont souvent aussi importants qu'une perte d'exploitation.

Les interdépendances de plus en plus nombreuses entre les machines, les entreprises et les fournisseurs, combinées à de faibles niveaux de stock, augmentent le risque d'une interruption d'activité et ses conséquences financières, et multiplient l'ampleur du sinistre en cas d'incident.

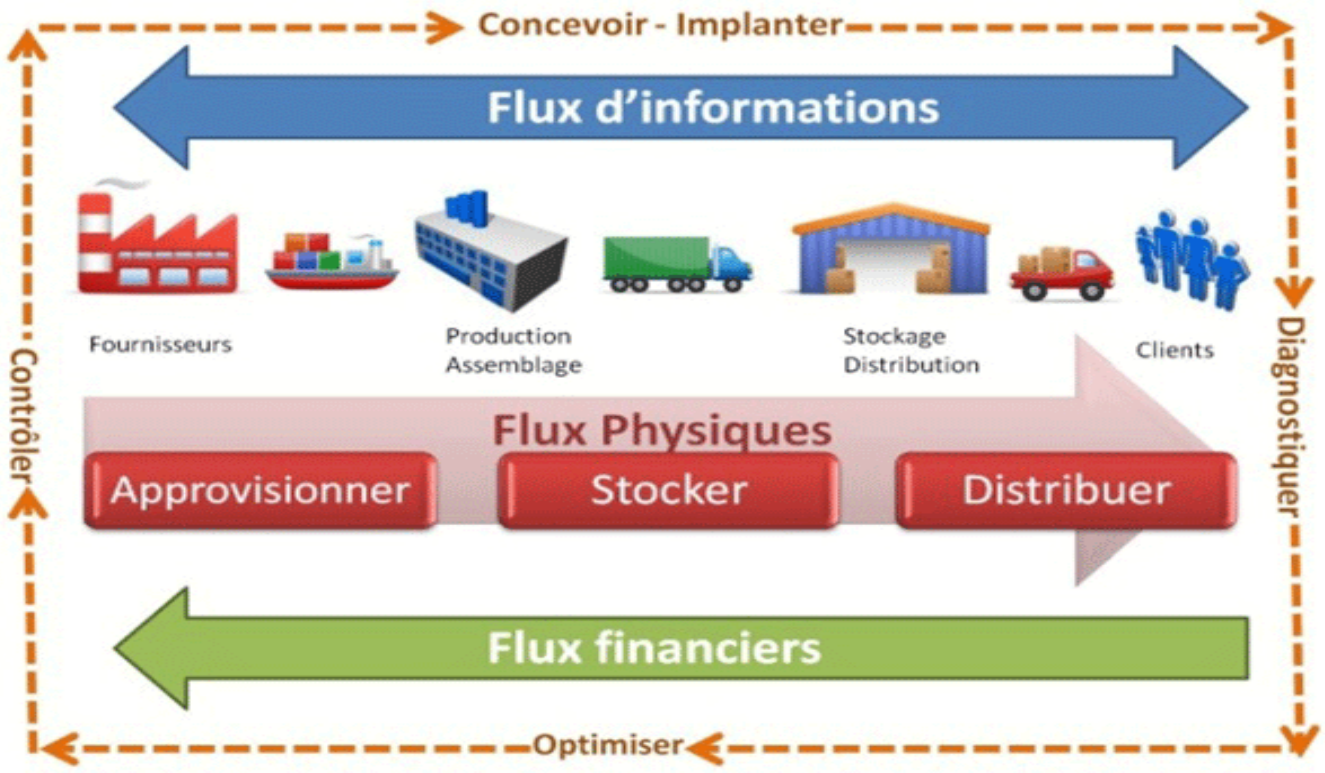
C'est aussi une menace que tout le monde ressent car les chaînes logistiques («supply chain») sont devenues tellement sophistiquées et tellement internationales que le moindre problème peut venir les perturber.

Il peut y avoir un chevauchement important dans les perturbations de la chaîne d'approvisionnement, les dommages de catastrophe naturelle et les événements de dommages non physiques. Ce chevauchement peut conduire à un effet multiplicateur au sein d'une entreprise.

Selon une étude annuelle du Business Continuity Institute, les trois principales causes de perturbation de la chaîne d'approvisionnement sont :

1. Pannes informatiques et télécoms
2. Cyberattaques et violation de données
3. Conditions météorologiques défavorables
4. La propagation d'une maladie contagieuse

Les autres causes d'interruption de la chaîne d'approvisionnement comprennent: les problèmes de transport, les problèmes de production, les grèves et les arrêts de travail, l'insolvabilité des fournisseurs et le risque politique. Bon nombre de ces causes de perturbation des fournisseurs sont liées à des dommages non physiques, elles peuvent donc ne pas être couvertes par les polices de dommages traditionnelles contre les pertes d'exploitation et, par conséquent, peuvent bénéficier d'une assurance de la chaîne d'approvisionnement large et spécifique offerte par certaines compagnies.



Cependant, il n'en demeure pas moins que de nombreux spécialistes de l'assurance supposent que la garantie PE est fournie par une assurance dommages aux biens, mais cette vision n'est plus appropriée pour les entreprises d'aujourd'hui, qui veulent protéger les actifs immatériels (ainsi que le tangible) et qui font face à des risques pouvant toucher leurs chaînes d'approvisionnement (pas seulement dans leurs propres locaux). Pour ces entreprises, l'impact de l'interruption d'activité (y compris la rupture d'approvisionnement) est le risque majeur pour leur continuité

Les pertes en PE et CPE deviennent plus importantes et plus complexes à mesure que les chaînes d'approvisionnement deviennent plus allégées avec une plus grande concentration sur un plus petit nombre de fournisseurs, en particulier dans des secteurs comme l'automobile, l'électronique et la pharmacie. Un événement tel qu'un petit incendie dans ces industries peut entraîner d'énormes pertes, par exemple une pénurie de pièces pour un constructeur automobile, la fabrication doit donc s'arrêter et des pertes dans la chaîne d'approvisionnement sont générées.

Evolution des risques d'Interruption des activités sans dommages matériels

L'analyse des sinistres met en évidence la pertinence croissante de la PE en tant que conséquence des pertes en assurance de biens, renforcée par l'environnement commercial de plus en plus interconnecté et mondialisé d'aujourd'hui. Presque toutes les grandes déclarations de sinistre en assurance de biens incluent désormais un élément PE majeur, qui représente généralement la majorité de la perte alors qu'auparavant la scission aurait pu être plus proche de 50:50.

De plus, les entreprises sont confrontées à un nombre croissant de scénarios de PE disruptifs à mesure que la nature du risque évolue dans la société connectée en réseau d'aujourd'hui. Beaucoup de ces scénarios peuvent se produire sans dommage physique mais avec des pertes financières élevées. La panne des systèmes informatiques, les cyber-incidents, les rappels de produits ou les incidents de qualité, les événements de terrorisme et de violence politique ou les émeutes, les incidents environnementaux ou de propagation des pandémies ou encore les changements réglementaires peuvent paralyser les opérations d'une entreprise et nuire gravement à sa capacité à fournir ses services, mais ils ne sont que l'un des nombreux déclencheurs de sinistres pouvant entraîner une PE pour les entreprises.

Dans le paysage politique et commercial incertain d'aujourd'hui, la PE peut émerger lorsque les entreprises sont confrontées à des problèmes environnementaux tels que la pollution sur un site de fabrication, sur des immeubles résidentiels ou par des déversements de pipelines. Il s'agit d'une exposition PE souvent négligée. Les dépenses et les perturbations de la chaîne d'approvisionnement peuvent augmenter rapidement en raison de longues mesures d'assainissement, de reconstruction et de retards au cours desquels les entreprises peuvent être incapables d'opérer ou de fournir des produits ou des services.

Aussi, les modifications de la réglementation et de la législation, telles que le départ prévu du Brexit par le Royaume-Uni de l'UE à la fin du mois de mars 2019, entraînent également un risque important en matière de PE sans dommage.

Le monde a fondamentalement changé au cours des dernières décennies, ce qui a conduit à une accumulation de risques et de nouveaux déclencheurs de sinistres PE.

PE sans dommages dans le contexte du COVID-19

Compte tenu de la perturbation sans précédent causée par l'épidémie de coronavirus, il n'est pas surprenant que l'interruption des activités et la pandémie soient en tête du baromètre des risques Allianz 2021.

Ces deux risques auxquels s'ajoutent les Cyber-risques sont interdépendants, démontrant les vulnérabilités croissantes et l'incertitude de notre monde hautement globalisé et connecté, où les actions en un seul endroit peuvent se propager rapidement pour avoir des effets mondiaux. Pour l'avenir, la pandémie montre que les entreprises doivent se préparer à un plus large éventail de déclencheurs d'interruption d'activité et d'événements extrêmes qu'auparavant. Il sera essentiel de renforcer la résilience des chaînes d'approvisionnement et des modèles commerciaux pour gérer les expositions futures.

Avant la pandémie, des entreprises individuelles, et même des secteurs entiers, ont subi d'importantes interruptions d'activité dans le passé, mais la pandémie de 2020 est le premier événement catastrophique à frapper une économie mondialisée et interconnectée moderne. Après la pandémie, la prise de conscience accrue du potentiel de pertes provenant à la fois des sources physiques traditionnelles d'interruption des activités et des déclencheurs de dommages non physiques, est au plus haut niveau.

La pandémie a démontré à quel point le monde est vulnérable aux événements imprévisibles et extrêmes et a mis en évidence les inconvénients de la production mondiale et des chaînes d'approvisionnement. Lorsque le transport par conteneurs a été effectivement immobilisé au printemps 2020, les flottes mettant de nombreux navires hors service en réponse à des pénuries de capacité, les chaînes d'approvisionnement mondiales ont été mises sous pression. Par la suite, les composants ne sont pas arrivés et la production s'est arrêtée dans de nombreuses industries.

Alors que le cyber était présumé l'une des causes potentielles d'interruption d'activité les plus préoccupantes, l'épidémie a démontré que l'interruption des activités est fortement corrélée à bon nombre des risques les plus préoccupants pour les entreprises aujourd'hui, tels qu'identifiés dans le baromètre des risques d'Allianz, tels que les catastrophes naturelles et le changement climatique, les risques politiques et les troubles civils, et même les changements rapides des marchés. La hausse des taux d'insolvabilité pourrait également affecter les chaînes d'approvisionnement.

L'une des grandes leçons tirées de la pandémie est que les événements extrêmes d'interruption d'activité ne sont pas seulement théoriques, mais une possibilité réelle.

Par exemple, une nouvelle souche de Covid-19 a même conduit à la fermeture soudaine des ports et des frontières britanniques fin décembre 2020, coïncidant avec la congestion portuaire existante pendant la période de Noël et la fin de la période de transition du Brexit.

Les conséquences de la pandémie sont également susceptibles d'augmenter les risques d'interruption des activités dans d'autres domaines engendrés par la poussée accélérée vers la numérisation, tandis que les répercussions économiques, sociétales et politiques de la pandémie pourraient également entraîner des perturbations pour les années à venir.

Par ailleurs, la dépendance croissante de la société à la technologie est une arme à double tranchant pour les interruptions d'activité. Etant un outil utile pour la continuité des activités, par exemple en passant au travail à distance et à la surveillance des processus ou à la vente et à la maintenance en ligne, il comporte également de nouveaux risques de perturbation plus graves lorsque la technologie sous-jacente tourne mal. La numérisation augmente la transparence de la chaîne d'approvisionnement, ce qui signifie que les organisations peuvent réagir plus rapidement et mieux, Cependant, une panne technique provoquant une panne majeure pourrait entraîner un événement d'interruption d'activité grave.

Un changement positif à émerger de la pandémie est une reconnaissance croissante de la nécessité de mieux gérer la mondialisation et de construire plus de chaînes d'approvisionnement résilientes.

Une résilience accrue des chaînes d'approvisionnement aidera non seulement à assurer l'assurabilité des risques liés à la chaîne d'approvisionnement, mais aidera également les clients à réagir plus rapidement aux tendances du marché.

Dans cette attente, les compagnies d'assurances ont pris les devants pour faire évoluer leurs conditions générales aux fins d'une exclusion claire du risque de pandémie et proposer de nouveaux régimes d'assurance couvrant ce type d'évènement exceptionnel, s'inspirant des solutions trouvés pour les catastrophes naturelles et le terrorisme.

Les poursuites en interruption d'activité COVID-19 : Les assureurs combattent sur tous les fronts

Des entreprises du monde entier ont été affectées par d'importantes perturbations ou fermetures en raison de la pandémie de coronavirus. Cela avait conduit à d'énormes pertes financières en plus d'autres difficultés économiques et personnelles. De nombreuses entreprises ont fait des déclarations de sinistres pour tenter de récupérer ces pertes financières dans le cadre de leurs polices d'assurance Interruption d'activité PE.

D'ailleurs, en 2020, la majorité des sinistres déclarés au titre des polices d'assurance contre les pertes d'exploitation par les assurés subissant des pertes en raison du COVID-19 ont été rejetées par les assureurs, débattant de la signification de certains termes de la police.

Aussi, plusieurs assureurs affirment que les pertes liées à la pandémie pourraient être les plus importantes de leur histoire et que les déclarations pour interruption d'activité en font majeure partie, même pour ceux qui ont prévu des exclusions de maladies contagieuses au cours de la dernière décennie après l'épidémie de SRAS en 2003.

La plupart des cas rejetés jusqu'à présent comportaient des clauses d'exclusion. Lorsque les polices ne sont pas exclues, les assureurs soutiennent que Les polices d'assurance commerciale sont destinées à couvrir les choses physiques et que le COVID-19 ne peut pas causer des dommages physiques ou des pertes d'exploitation, comme une tornade ou une inondation. Cet argument parait fort et pourra éventuellement plaider en faveur de l'industrie dans la bataille juridique sur la couverture.

La préoccupation universelle se concentre sur le manque de clarté concernant la signification de certains termes des polices Pertes d'exploitation, le résultat de ces sinistres et la façon dont le secteur de l'assurance prend des décisions à leur égard. Cette incertitude a conduit certains régulateurs à intervenir pour résoudre l'ambiguïté contractuelle concernant ces allégations età porter en fait un cas type devant les tribunaux pour déterminer comment le libellé des politiques devrait être interprété.

Les avocats de quelques assurés se sont donc attaqués à l'ambiguïté du wording des exclusions, en statuant le manque de précision pour l'exclusion des sinistres causés par «la présence de champignons, de pourriture humide, de pourriture sèche, de bactéries ou de **virus**». Ils estiment que refuser la couverture des pertes COVID-19 ne correspond pas logiquement aux autres polluants de base tels que prévus par la police.

D'autres avocats ciblent les instructions de verrouillage de l'État comme un moyen de contourner les problèmes montrant que le virus a physiquement endommagé les entreprises de leurs clients. Mais pour obtenir une indemnisation au titre de la garantie PE, ils doivent prouver que c'est le virus qui avait causé les dommages tangibles.

Malgré les revers, les assurés ne voient aucune solution pour compenser les dégâts causés par l'interruption de leurs activités suite Covid-19, que de revendiquer indemnisation au titre de leurs polices d'assurance PE. De leur côté, les assureurs se préparent aux recours collectifs en cas d'interruption d'activité.

Cela n'empêche que les assureurs sont convaincus de constituer des réserves pour sinistres dans l'attente de déclarations PE des entreprises touchées par les confinements et les interruptions d'activités. Mais comme les sinistres sont en grande partie comptabilisées sur une base encourue, mais non déclarée, et pourraient être libérées si les affaires judiciaires sont tranchées en faveur des assureurs.

Il a également été laissé entendre qu'entre 1 et 1,4 milliard de dollars avaient été payés par Lloyds pour des sinistres pour interruption d'activité en raison d'un coronavirus, malgré le fait que la grande majorité des entreprises n'avaient pas la bonne couverture et la bonne protection en vigueur pour ce type d'événement «.

Le coût ultime dépendra de l'issue des litiges en cours ou futurs et des sinistres potentiels découlant de futurs verrouillages. Il est prévu que le risque d'ambiguïté diminuera au fur et à mesure que les polices seront renouvelées, et les assureurs actualiseront leurs wording des polices et stipuleront clairement les exclusions en cas de pandémie.

Fitch Ratings a révélé que les déclarations de sinistres PE sont probablement la plus grande source de réclamations liées à la pandémie COVID-19 qui pèsent sur les revenus des assureurs non-vie et a aussi averti que l'incertitude concernant les PE s'ajoutait à la pression existante sur les bénéfices des assureurs non-vie, le bénéfice net du secteur passant de 3,4 milliards de dollars au cours des 12 mois précédents à 0,9 milliard de dollars au cours des 12 mois clos en septembre 2020 en raison d'une baisse significative en revenus des placements.

Royaume-Uni : la Cour suprême statue sur les réclamations d'assurance contre les pertes d'exploitation COVID-19

En juin 2020, la Financial Conduct Authority (FCA) a porté une affaire test devant la High Court, dans le but de fournir une certitude tant aux assureurs qu'aux assurés. L'affaire était basée sur 21 police types émises par huit assureurs: Arch Insurance (UK) Ltd, Argenta Syndicate Management Ltd, Ecclesiastical Insurance Office Plc, MS Amlin Underwriting Ltd, Hiscox Insurance Company Ltd, QBE UK Ltd, Royal & Sun Alliance Insurance Plc, Zurich Insurance Plc.

Le tribunal a été invité à examiner les trois types les plus courants des conditions de police d'assurance en cas d'interruption des activités:

TYPE 1 : couverture pour Perte d'exploitation causée par un foyer de maladie à proximité des locaux

TYPE 2 : couverture pour interruption d'activité causée par la prévention de l'accès aux locaux, suite à une action de l'autorité publique, prise en raison d'une urgence ;

TYPE 3 : Forme «hybrides» combinant à la fois une exigence pour l'apparition de la maladie et le refus de l'autorité publique d'accéder aux locaux.

L'arrêt de la Cour suprême a été rendu le 15 janvier 2021, a résolu un certain nombre d'incertitudes contractuelles et de problèmes liés à la causalité, et apporte une bien plus grande clarté tant aux assurés qu'aux assureurs sur l'efficacité de la couverture, la validité des sinistres et les montants dus aux assurés.

Son arrêt long et complexe a principalement abordé les points suivants :

1. L'interprétation des «clauses de maladie»
2. L'interprétation des clauses de «prévention de l'accès»
3. La question de savoir quel lien de causalité doit être établi entre les pertes liées à une interruption d'activité et la survenue d'une maladie à déclaration obligatoire
4. L'effet des «clauses de tendances»
5. L'importance dans la quantification des pertes liées à une interruption d'activité des effets de la pandémie sur l'activité survenus avant le déclenchement de la couverture.

Enfin, la Cour suprême a statué que:

TYPE 1 : Clause maladie, couverture était disponible et pouvait être satisfaite par des événements individuels. Bien que la Cour suprême ait interprété les clauses relatives aux maladies plus étroitement que la Haute Cour, sa décision sur les questions de causalité visées au point c) ci-dessous signifiait que cela n'affectait pas le principe général selon lequel ces clauses relatives aux maladies pouvaient couvrir les pertes résultant d'épidémies localisées de la maladie à déclaration obligatoire en combinaison avec la pandémie plus large, même si cette épidémie localisée à elle seule n'aurait pas suffi à provoquer des pertes pour les assurés.

Les TYPES 2 et 3 peuvent être disponibles pour la fermeture partielle ou complète d'une entreprise ou l'accès à une partie des locaux ainsi que pour les ordres de fermeture obligatoires qui n'étaient pas juridiquement contraignants. Une véritable étape législative ordonnant la clôture n'est pas requise.

Les sinistres valides ne devraient pas être réduits au motif que la perte aurait résulté en tout cas de risques non assurés résultant de la pandémie. Les assureurs avaient fait valoir que la nature généralisée de la pandémie aurait inévitablement entraîné des pertes commerciales même si l'un des événements assurés (c'est-à-dire la survenance d'une maladie dans un rayon spécifié ou une action des autorités publiques empêchant l'accès aux locaux) ne s'était pas produit. La Cour suprême a rejeté cette interprétation et a statué que la police serait déclenchée lorsque le risque assuré, combiné à tout risque non assuré similaire, entraînait une perte.

La décision ne signifie pas une acceptation globale des sinistres PE, et les assureurs ne seront pas responsables des paiements lorsque les polices contiennent déjà des exclusions explicites. Les réclamations devront encore être examinées individuellement contre la décision de la Cour suprême et les pertes devront être prouvées.

Cependant, le jugement rendra plus difficile pour les assureurs de refuser la couverture ou de réduire les paiements au motif que des pertes auraient résulté en tout état de cause de risques non assurés dont la cause sous-jacente est la pandémie. Un plus grand nombre de titulaires de police d'assurance contre les pertes d'exploitation auront des sinistres valides, et certaines indemnisations seraient plus élevées que ce qui avait été précédemment reconnu.

Conclusion

Il y avait «des leçons assez dures» à tirer de la pandémie, et le marché de l'assurance devrait à l'avenir structurer les polices et les couvertures Pertes d'exploitation différemment afin que les entreprises soient «mieux protégées». Après, restent encore des dilemmes qui pourraient donner lieu à de nouveaux litiges. Par exemple, la question de l'agrégation et si les assureurs devraient accepter que la perturbation causée par la pandémie soit un événement ou plus.

En effet, le secteur de l'assurance ne peut pas relever tous les défis, mais peut, en partenariat avec les clients, garantir certains des plus grands facteurs d'interruption d'activité, tels que les catastrophes naturelles et les incendies, ainsi que certains cyber-incidents et d'offrir des services d'ingénierie des risques et des solutions alternatives de transfert des risques pour soutenir les économies en ces temps difficiles.

Risques Emergents

5. Terrorisme

Le terrorisme est un phénomène complexe qui a des répercussions sur tous les aspects de la société et est devenu au fil du temps une menace qui ne connaît pas de frontières géographiques.

Bien qu'ils existent plusieurs définitions du terrorisme, on peut convenir que le terrorisme cherche à causer des souffrances humaines et une peur généralisée à des fins politiques, idéologiques, religieuses ou économiques.

Les coûts économiques du terrorisme sont au plus haut niveau depuis l'année 2001. En effet, Le terrorisme est en constante évolution et s'adapte aux changements de l'environnement sociopolitique mondial. Certains de ces changements facilitent la capacité des terroristes à opérer, à obtenir des fonds et à développer de nouvelles capacités. La technologie des armes est devenue de plus en plus disponible et le pouvoir d'achat des organisations terroristes est en augmentation. La disponibilité immédiate de la technologie et du personnel qualifié pour la faire fonctionner permet au terroriste bien financé d'égaler ou de dépasser la sophistication des contre-mesures gouvernementales.

FIGURE 1 Little change in the countries at highest risk from May 2018 to May 2019.

SOURCE: WORLD RISK REVIEW

Terrorism

May 2018	May 2019
1. Afghanistan	1. Afghanistan
2. Yemen	2. Syrian Arab Republic
3. Iraq	3. Libya
4. Syrian Arab Republic	4. Yemen
5. Somalia	5. Iraq

Strikes, riots, and civil commotion

May 2018	May 2019
1. Venezuela	1. Venezuela
2. Yemen	2. Yemen
3. South Africa	3. South Africa
4. Bangladesh	4. Zimbabwe
5. Bolivia	5. Iraq

War and civil war

May 2018	May 2019
1. Syrian Arab Republic	1. Syrian Arab Republic
2. Afghanistan	2. Afghanistan
3. South Sudan	3. Yemen
4. Yemen	4. Libya
5. Libya	5. South Sudan

Le terrorisme n'est pas alors un phénomène nouveau mais c'est un risque dont les mécanismes par lesquels il opère sont en développement continu ce qui justifie la considération de ce risque comme étant un risque émergent.

Jusqu'à récemment, le terrorisme était principalement associé à des actes de violence physique et à des crimes, tels que les meurtres, les attentats à la bombe, les enlèvements et la destruction de biens. De nos jours et avec l'avènement croissant de la technologie, et plus particulièrement des systèmes contrôlés par des ordinateurs, on assiste à une nouvelle forme d'activité criminelle qui a souvent combiné la destruction de biens avec la criminalité financière, la propagande, la guerre économique en plus des dommages physiques à des vies innocentes.

Le cyber-terrorisme est l'une de ces nouvelles formes de criminalité et qui est associé à des individus, des groupes terroristes et des acteurs étatiques ce qui, en particulier, pourrait dégénérer en une «cyber-guerre». Le cyber-terrorisme permet aux terroristes de mener leurs opérations avec peu ou pas de risque pour eux-mêmes. Il offre également aux terroristes la possibilité de perturber ou de détruire des réseaux et des ordinateurs. Le résultat est l'interruption des principales activités gouvernementales ou commerciales. Ce type de terrorisme n'est pas aussi médiatisé que d'autres types d'attentats terroristes, mais son impact peut être très destructeur.

En effet, l'utilisation accrue des réseaux sociaux comme outil de recrutement des terroristes combiné à un accès accru à ces réseaux et autres moyens de communications mobiles, l'intensification des conflits régionaux et internationaux et le recours élargi à la cyber-guerre par les États contribuent de manière continue à l'évolution et l'aggravation de ce phénomène.

Depuis les attentats du 11 septembre 2001, les mesures et actions de lutte contre le terrorisme dans le monde se sont développées et renforcées. Les attaques de cette ampleur n'ont pas été répétées jusqu'à présent. Cependant, il y a eu un nombre croissant d'attaques plus discrètes et non sophistiquées qui sont plus difficiles à détecter, où les soi-disant loups seuls agissent au nom de groupes terroristes. Plus important encore, la fréquence de ces attaques a augmenté au cours de la dernière année et la cible des attaques s'est déplacée vers des cibles non évidentes ou douces comme les boîtes de nuit (Paris, Orlando), les lieux de travail (Oregon), les plages (Tunisie)…

L'assurance du risque Terrorisme :

Pour le secteur de l'assurance, la violence politique et le terrorisme sont difficiles à gérer, car la fréquence et la gravité des attaques ne peuvent être prédites. En outre, les organisations militantes et terroristes mondiales d'aujourd'hui cherchent constamment à accroître l'ampleur de leurs attaques en acquérant et en déployant des armes non conventionnelles comme des agents nucléaires, biologiques, chimiques ou radioactifs. Habituellement, les polices qui couvrent les risques politiques et le Terrorisme et les traités de réassurance excluent les pertes résultant d'une attaque via des dispositifs nucléaires, biologiques, chimiques ou radioactifs. Cela est dû au risque incalculable et au potentiel de perte résultant de telles attaques.

Par ailleurs, et en plus de la population civile, des intérêts militaires, policiers et gouvernementaux, les actes terroristes touchent aussi les entreprises et les différents intervenants du secteur économique. En effet, certains secteurs économiques ont été particulièrement ciblés, y compris le tourisme, les transports, le commerce de détail, les industries d'extraction, les infrastructures essentielles et le secteur financier. De telles attaques peuvent aussi se traduire par des coûts indirects pour les entreprises en provoquant l'interruption de leurs activités.

Afin d'atténuer les impacts économiques plus larges (en raison du manque de couverture d'assurance complète pour les biens commerciaux ou les infrastructures), de nombreux gouvernements ont mis en place des mécanismes d'assurance et de réassurance contre le terrorisme soutenus par l'État appelés fonds ou pools de terrorisme.

Les différents programmes antiterroristes reflètent les besoins particuliers de chaque pays et la plupart diffèrent par leur structure ou leur application.

Cependant, et en raison de plusieurs crises politiques et des actes terroristes récents, la demande de couverture de ce risque ne cesse d'augmenter. A cet effet, les assureurs continuent à développer et proposer des solutions nouvelles et innovantes aux professionnels qui sont appelés à adopter de nouvelles stratégies pour protéger leurs propriétés, leurs employés et leurs affaires.

Avant les événements du 11 septembre 2001 aux États-Unis, les risques terroristes étaient souvent couverts par des assureurs privés ou du moins pas spécifiquement exclus en assurance de biens.

Après ces événements, il y a eu de nombreux changements sur le marché mondial de l'assurance contre le terrorisme avec une tendance des assureurs mondiaux à exclure cette couverture de leurs contrats.

Les sinistres couverts qu'ont entraînés les attentats du 11 septembre 2001 totalisent environ 32,5 millions de dollars . Puisque la majeure partie des coûts financiers associés aux attentats ont fini par être assumés par les réassureurs et que, par la suite, plusieurs d'entre eux se sont retirés du marché, les assureurs ont fini par exclure le risque terroriste de leurs polices d'assurance. Les entreprises ne pouvaient donc plus se procurer d'assurance contre le terrorisme. En 2002, afin « d'assurer le maintien de l'offre à coût raisonnable de garanties d'assurance pour entreprises contre les dommages matériels dus au terrorisme, et afin de permettre au marché du secteur privé de se stabiliser et d'être en mesure d'absorber de nouveaux sinistres résultant d'actes terroristes », le Congrès américain a promulgué le Terrorism Risk Insurance Act (TRIA).

Le TRIA exigeait essentiellement que les assureurs offrent des garanties d'assurance aux entreprises contre les dommages matériels résultant d'actes officiellement reconnus en tant qu'attentats terroristes et que soient mis en place « des modes de compensation partagés entre les secteurs privé et public pour couvrir les sinistres couverts de cette nature ». En réalité, le TRIA a fait du gouvernement américain un assureur de dernier recours, c'est-à-dire un partenaire dont les réserves financières aident à régler les demandes d'indemnité en cas d'attentats terroristes de grande envergure, mais seulement après que les entreprises et les assureurs concernés aient payé les franchises qu'ils doivent assumer. Par conséquent, les assureurs américains doivent inclure des garanties d'assurance contre le terrorisme dans toutes leurs polices d'assurance de dommages et les modalités de ces garanties doivent être sensiblement semblables à celles des garanties couvrant d'autres risques.

La portée du TRIA a été élargie en 2007, puis en 2015, quand cette loi a pris le titre de : Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA). Les principaux facteurs pouvant déclencher l'application des dispositions du TRIPRA sont les suivants :

- L'événement de nature terroriste doit répondre à la définition d'acte terroriste,

- L'acte terroriste doit être officiellement reconnu comme admissible en vertu de la loi par le Département du Trésor des États-Unis, après entente avec le secrétaire d'État et le procureur général, et en consultation avec le secrétaire à la Sécurité intérieure des États-Unis,

- L'événement de nature terroriste doit avoir entraîné des pertes qui excèdent le seuil d'indemnisation prescrit (140 millions de dollars en 2017).

Fait à noter, jusqu'à ce jour, le TRIPRA n'a versé aucune indemnité parce qu'aucun acte de terrorisme n'a officiellement été reconnu comme tel par les autorités responsables.

Cependant, les entreprises peuvent souscrire une police d'assurance des biens distincte contre les dommages dus au terrorisme. Les avantages les plus évidents que procure une telle police distincte sont que la définition n'est pas limitée aux incidents qui sont officiellement reconnus par les gouvernements et que le montant de la garantie souscrit peut couvrir la totalité des pertes subies.

Une police d'assurance distincte contre le terrorisme est avantageuse aussi parce que la définition d'acte terroriste qu'elle comporte peut-être assez large. Les montants de garantie offerts dans les polices distinctes sont aussi souvent plus élevés que ceux prévus dans un avenant.

Evaluation du risque terroriste par l'assureur / réassureur :

Plusieurs secteurs pourraient potentiellement être confrontés à des pertes financières importantes du fait du terrorisme :

- Ménages et entreprises dont la couverture d'assurance est insuffisante.

- Compagnies d'assurance et de réassurance incapables de se réassurer ou de transférer les risques sur les marchés des capitaux.

- Les gouvernements fournissant un soutien au marché de l'assurance contre le terrorisme.

En outre, le changement de style d'attaque terroriste nécessite également un changement d'orientation de l'assurance. Si les réclamations pour dommages matériels à grande échelle devraient être moins fréquentes, elles restent importantes en termes généraux. Cependant, les réclamations pour interruption d'activité et responsabilité civile deviennent de plus en plus une priorité. Là où l'interruption d'activité serait généralement vendue parallèlement à l'assurance des biens, les assureurs commencent à envisager d'incorporer les dommages non matériels dans leurs forfaits de terrorisme.

Les définitions du terme « terrorisme » qui sont typiquement incluses aux contrats d'assurance n'englobent pas les risques de nature politique et ne couvrent pas les dommages découlant de grèves, d'émeutes, de mouvements populaires, de rébellions, de révolutions, de guerres, d'insurrections ou de cyberterrorisme. Mais, il existe des contrats qui comportent des définitions plus étendues.

La cybersécurité est également sensible aux interventions terroristes et une attaque de cyber-terrorisme à grande échelle est toujours redoutée. Le piratage informatique parrainé par l'État continue de susciter des inquiétudes. En outre, les infrastructures critiques, y compris les centrales nucléaires, sont de plus en plus ciblées par des pirates non affiliés à des groupes terroristes dans l'intention de causer des dommages aux produits, aux entreprises et aux personnes. Le potentiel de perte de vie existe, ce qui amplifie la portée des risques d'assurance.

Pour en arriver à gérer le risque terroriste, les assureurs / réassureurs doivent d'abord comprendre dans quelle mesure l'entreprise à assurer est exposée à ce risque et à d'autres types d'événements similaires, et ensuite évaluer l'importance de cette exposition.

Les assureurs / réassureurs doivent tenir compte des facteurs suivants au moment d'évaluer l'exposition de l'entreprise à assurer au risque terroriste :

- l'intérêt que présente l'entreprise ou son emplacement en tant que cible pour les terroristes : il faut examiner la nature et l'emplacement de l'entreprise, les caractéristiques de ses propriétaires, le nombre de personnes fréquentant les lieux, l'intérêt que présentent les entreprises adjacentes, etc.

- l'intérêt que présentent certains actifs ou certaines installations de l'entreprise : il faut prendre en considération le niveau de sécurité, l'accessibilité des entrées, la solidité des structures, les plans d'évacuation…

- les risques financiers : il faut étudier le risque auquel est exposé le capital de l'entreprise, les retombées financières liées à l'interruption des activités pour cause de dommages directs et collatéraux, les franchises et les montants de garantie requis, etc.

Il existe un certain nombre d'outils et de modèles analytiques pouvant aider les assureurs à évaluer l'exposition de leurs clients au risque terroriste et à déterminer les montants de garantie dont ils ont besoin avec, bien sûre, l'aide des experts en la matière.

Que couvre l'assurance contre le terrorisme ?

1. Assurance simple contre le terrorisme

L'assurance contre le terrorisme couvre la perte ou les dommages aux biens assurés et la perte de revenus consécutive à des actes de terrorisme et de sabotage.

2. Assurance contre la violence politique

Cette police offre une couverture contre la perte ou les dommages aux biens assurés et la perte de revenus consécutive à des actes de terrorisme et de sabotage en y ajoutant certaines extensions. Ce type de police étend la couverture aux :

- Émeutes, grèves et / ou agitation civile
- Dommages malveillants
- Insurrection, révolution ou rébellion
- Mutinerie et / ou coup d'état
- Guerre et / ou guerre civile

2. Produits étendant la portée de l'assurance contre le terrorisme

À mesure que les attaques terroristes évoluent et deviennent de plus en plus diversifiées, la demande pour de nouveaux types de garanties adaptées augmente. Ainsi, bien que les dommages matériels résultant d'une attaque terroriste puissent être relativement limités (notamment si on les compare aux dommages subis lors des attentats du 11 septembre 2001), les frais devant être assumés par une entreprise dont les activités sont interrompues en raison d'une attaque d'envergure restreinte pourraient tout de même atteindre des montants considérables.

De même, si un gouvernement décrète le couvre-feu dans une région donnée ou en empêche l'accès, les activités des entreprises établies dans cette région pourraient être perturbées pendant une période indéfinie.

Voici quelques produits offerts dans ce cadre qui étendent la portée de l'assurance contre le terrorisme :

- Pertes d'exploitation
- Frais d'évacuation supplémentaires en cas de menace
- Annulation de réservations
- Annulation d'événements
- Dispositifs chimiques, biologiques, radiologiques et nucléaires (CBRN) : Cette garantie couvre les risques tels que les attaques mettant en cause l'anthrax, le ricin, les virus et les « bombes sales » (p. ex., une personne en possession de matériaux radioactifs expose d'autres personnes aux radiations).

- Situations mettant en cause un assaillant actif : il s'agit d'un type de garantie relativement nouveau qui couvre les incidents impliquant des personnes qui pénètrent dans la propriété d'un assuré en brandissant une arme quelconque et dont les gestes n'ont pas de connotation politique, qu'elle prévoit des indemnités pour les dommages matériels, les consultations psychologiques offertes aux survivants et la perte d'attractivité de la propriété, et qu'elle couvre même les frais engagés pour enquêter sur les menaces formulées à l'égard de l'assuré.

Tarification

Les primes sont généralement établies en fonction d'un pourcentage de la prime payée pour la police d'assurance des biens et elles correspondent habituellement à un faible pourcentage de celle-ci. Le pourcentage varie selon le secteur d'activité de l'assuré, la région où se situe le risque et son degré d'exposition à une attaque terroriste.

Le risque du terrorisme en Tunisie

Les évènements qu'a connu la Tunisie ces dernières années (mouvements populaires, actes de terrorisme) ont pesé lourdement sur l'économie tunisienne et ont affecté plusieurs entreprises et intervenants économiques en plus des pertes humaines.

En effet, et depuis la révolution Tunisienne du 14 Janvier 2011, la Tunisie a souffert d'une série d'attaques terroristes revendiquées par des organismes Djihadistes et qui ont ciblé les forces de l'ordre et l'armée tunisienne à plusieurs reprises.

En plus les actes terroristes ont visé les touristes notamment lors des attaques du Musée du Bardo et de la Plage de Sousse. Ces attaques ont été responsables de la mort de dizaines de soldats et de policiers, mais aussi de nombreux civils et de 59 touristes étrangers, dont une quarantaine à Sousse en 2015.

Ces attaques sanglantes ont affecté gravement l'économie du pays et bien particulièrement le secteur du Tourisme.

Heureusement, la situation sécuritaire du pays s'est nettement améliorée ces dernières années grâce aux efforts des différentes unités sécuritaires et militaires et on remarque une nette diminution des actes terroristes et de leur incidence et qui se limitent désormais à quelques attaques contre les forces de sécurité notamment dans les massifs montagneux frontaliers de l'Algérie.

Face à cette situation, les compagnies d'assurances tunisiennes conscientes de leur rôle de soutien à leurs clientèles et en réponse au besoin accru des différents intervenants économiques pour une couverture adéquate contre ce risque émergent, ont multiplié leurs efforts pour mettre en place une couverture qui prend en charge le risque du terrorisme et qui répond aux besoins des clients tout en s'inspirant des expériences des assureurs et réassureurs internationaux et des produits qu'ils proposent.

Ainsi, plusieurs compagnies ont commencé à offrir et commercialiser cette garantie sur le marché pour les différents secteurs d'activité à savoir l'hôtellerie, l'industrie, le commerce…

Par ailleurs, et en collaboration avec tout le secteur financier, les compagnies d'assurance tunisienne, la société Tunisienne de réassurance, la fédération tunisienne des sociétés d'assurances et le comité général des assurances ont contribué à la mise en place du système national de lutte contre le blanchiment d'argent et le financement du terrorisme et se sont engagés pour se conformer aux exigences réglementaires en la matière.

Risques Emergents

6. Risque de changement de normes comptables et prudentielles

Devant les changements de normes comptables et du référentiel prudentiel notamment IFRS 17, et les nouvelles recommandations sur Solvabilité 2, les assureurs sont de plus en plus exposés à des risques règlementaires dont les enjeux dépassent de loin les aspects comptables.

Oui l'existence d'un référentiel de normes uniques facilite la lisibilité et la comparabilité des comptes et par conséquent constitue un facteur de confiance additionnel pour l'investisseur permettant de renforcer la confiance, de stimuler l'investissement et favoriser le développement et la croissance des entreprises. Mais Il va induire de profonds bouleversements en matière de communication financière des groupes d'assurance et il aura des conséquences majeures sur l'organisation du pilotage de la performance. En outre, l'impact opérationnel sur les données, les systèmes et les process sera considérable.

IFRS 17 : redéfinit la comptabilisation des contrats d'assurance

L'IASB (International Accounting Standard Board) a publié le 25 juin 2020 le texte définitif de la norme IFRS 17, Contrats d'assurance dont la version initiale a été publiée le 18 mai 2017. IFRS 17 établit les principes pour la comptabilisation, l'évaluation et la présentation des contrats d'assurance. La révision de la norme vise à répondre aux préoccupations des parties prenantes, en particulier sur le report de la date d'application au 1er janvier 2023 et sur les mismatchs comptables.

Ces amendements portent sur les sujets principaux suivants :

Champ d'application de la norme IFRS 17

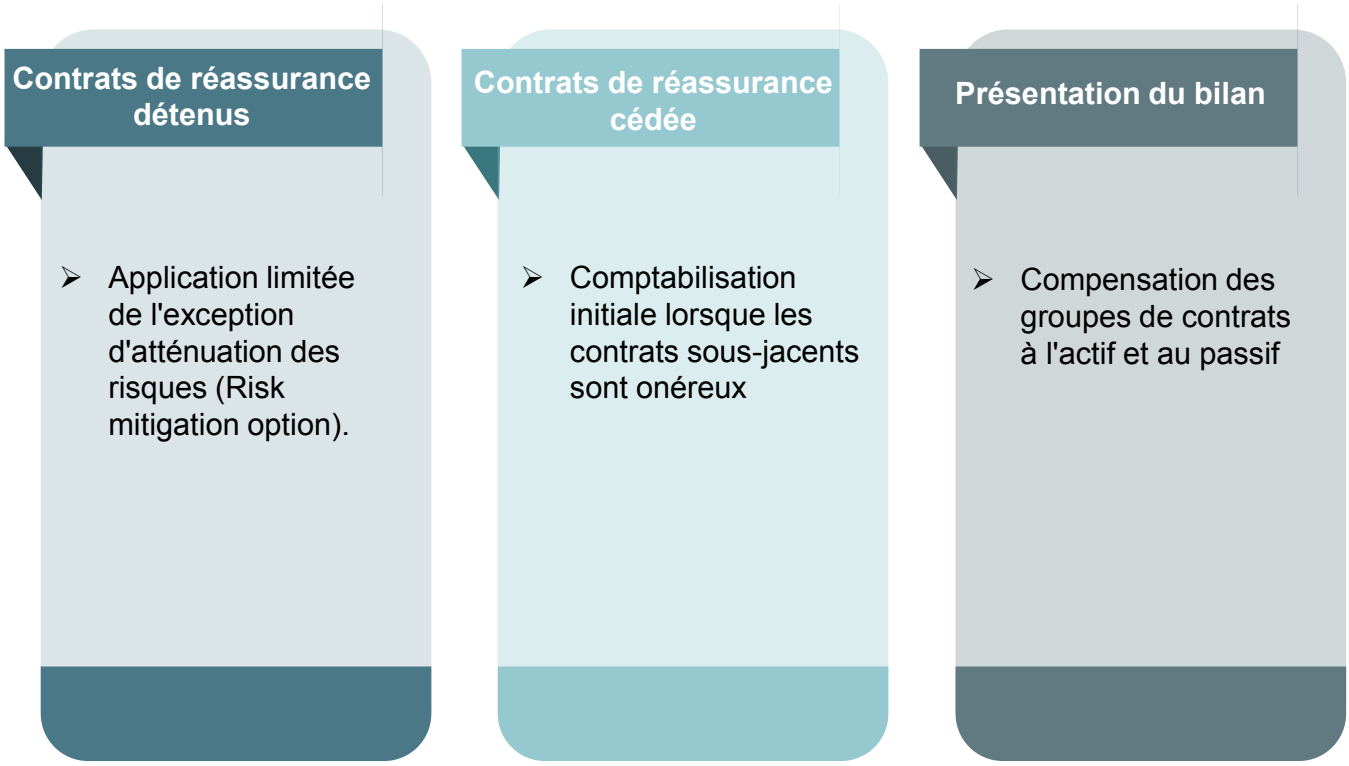
- Exclsion du champ d'application de IFRS 17 les contrats dont l'objet principal est l'octroi de prêts et autres formes de crédit.

Flux de trésorerie liés aux frais d'acquisition des contrats

- Permettre à l'entité d'allouer une part des frais d'acquisition payés aux renouvellements futurs attendus.

Marge de services contractuels

- Le service d'investissement (service de rendement d'investissement pour les contrats du modèle général) est un service du contrat d'assurance.
- les unités de couverture doivent refléter la quantité de prestations fournies au titre des différents services du contrat d'assurance.



Rappel de la norme IFRS 4 Norme en vigueur pour les contrats d'assurances jusqu'au 1er janvier 2023

La norme IFRS 4 est consacrée aux contrats d'assurance y compris les traités de réassurance, c'est une norme transitoire qui reste en vigueur jusqu'au 1er janvier 2023 date d'entrée en vigueur de IFRS 17.

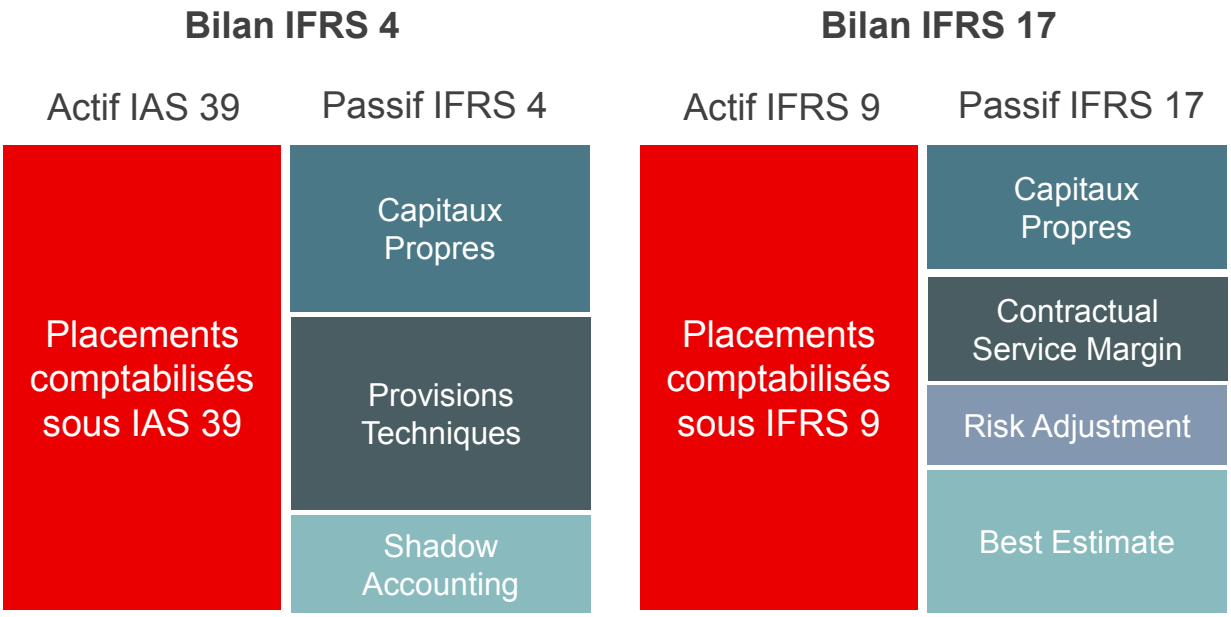
L'objectif ultime d'une norme spécifique aux contrats d'assurances est la valorisation des passifs d'assurance à la juste valeur. Toutefois, la norme IFRS 4 a limité les retraitements apportés aux normes comptables locales en vigueur. En effet, les assureurs peuvent continuer à évaluer les passifs d'assurance au coût amorti ou au coût historique ce qui ne respecte pas le cadre conceptuel des IFRS. Dans ces conditions, l'objectif de comparabilité entre les assureurs ne peut pas être atteint.

Néanmoins, elle a apporté des garde-fous en imposant un test de suffisance des passifs d'assurance ou Liability Adequacy Test, LAT pour s'assurer de la non sous-évaluation des passifs d'assurance dans le cadre du maintien du référentiel comptable existant. Ce test suppose que l'assureur évalue à chaque date de reporting si ses passifs d'assurances comptabilisés sont suffisants en utilisant les estimations actuelles de flux de trésorerie futurs générés par ses contrats d'assurance.

Si cette évaluation indique que la valeur comptable de ses passifs – diminuée des coûts d'acquisitions différés et des immobilisations incorporelles liées – est insuffisante au regard des flux de trésorerie futurs estimés, l'insuffisance totale doit être comptabilisée en résultat.

Un test de dépréciation relatif aux actifs au titre de cessions en réassurance est aussi imposé. Autre mesure garde-fou, IFRS 4 interdit les provisions au titre des demandes d'indemnisation éventuelles selon des contrats d'assurance non encore souscrits à la date de reporting telles que les provisions pour égalisation.

Pour l'assurance vie, la norme a prévu la mise en place de la comptabilité reflet ou shadow accounting, mécanisme permettant de réduire le mismach comptable du à l'inadéquation entre actifs valorisés à la juste valeur (IFRS 9 et IAS 39) et passifs valorisés au coût amorti (IFRS 4) par l'affectation d'une partie de la revalorisation comptable des actifs aux assurés vie via la comptabilisation au passif de participation bénéficiaire différée.



IFRS 17 La Norme définitive spécifique aux contrats d'assurance

Après un marathon de discussions et d'exposé-sondages divulgués par l'IASB, la norme définitive spécifique aux contrats d'assurance IFRS 17 a été publiée le 18 mai 2017 pour venir remplacer la norme actuellement en vigueur et résoudre ses limites. Elle entrera en vigueur le 1er janvier 2023 avec une année comparative 2022 retraitée.

Les changements envisagés dans cette norme conjugués à ceux d'IFRS 9 s'apparentent pour les assureurs à une deuxième conversion aux IFRS. Ils constituent une véritable révolution pour le secteur, bien plus qu'une simple évolution de normes comptables.

La nouvelle norme est fondée sur des fondamentaux proches de ceux de la directive Solvabilité 2, tels qu'une évaluation du passif d'assurance basée sur une vision prospective des flux de trésorerie en juste valeur. Toutefois, des divergences demeurent, telles que :

- Le périmètre des flux du Best Estimate (BE) ;

- La Risk Margin (RM) sous S2, laisse place au Risk Adjustment (RA) sous IFRS 17 ;

- Le passif IFRS 17 introduit une nouvelle composante : la Marge de Service Contractuelle (CSM).

Une synergie entre solvabilité 2 et IFRS 17 est de nature à permettre aux assureurs de rationaliser les processus de production des reportings prudentiels et comptables et de faciliter les réconciliations et les contrôles.

Granularité des calculs

La norme IFRS 17 exige une maille fine pour l'évaluation des contrats d'assurance et la publication des comptes. Toutefois, elle accepte de regrouper des contrats respectant les conditions suivantes :

- Les contrats sont souscrits sur une période d'un an maximum ;

- Les contrats correspondent à des garanties similaires ;

- Ils ont le même statut de profitabilité attendue à la souscription : profitable, onéreux ou profitable mais susceptible de devenir onéreux.

Ce principe a été imposé par l'IASB afin de ne pas agréger des générations de contrats qui ne sont pas ou plus profitables avec de nouvelles générations de contrats profitables. Au sein de chaque cohorte annuelle, les contrats sont également segmentés en tenant compte de leur profitabilité attendue à la souscription : les contrats profitables ne pourront pas compenser les contrats déficitaires.

La norme ne permet pas de changer ou remettre en question le regroupement des contrats une fois la première comptabilisation a été réalisée.

La segmentation des portefeuilles représente ainsi l'une des difficultés majeures liées à la comptabilisation des passifs des contrats d'assurances.

Les exigences de la norme IFRS 17 en termes de segmentation, soulèvent de nombreuses problématiques d'ordres métier, méthodologique et opérationnel. IFRS 17 conduit les assureurs à se doter de nouvelles métriques pour évaluer la profitabilité des contrats, et ce, sur un niveau de granularité relativement fin. Ceci fait ressortir de véritables enjeux autour de la spécification de la profitabilité qu'il appartient à chaque assureur de définir, en sélectionnant les indicateurs de rentabilité les plus pertinents (e.g. CSM par cohorte, ratio combiné IFRS 17 intégrant un «RA de prime»,...) ainsi que les méthodes les plus adéquates pour circonscrire ces nouveaux indicateurs, comme par exemple l'usage de scénarii adverses permettant de détecter des contrats potentiellement onéreux.

Le niveau de segmentation des calculs IFRS 17 soulève des problématiques opérationnelles d'augmentation des temps de projection et des enjeux méthodologiques comme par exemple l'allocation à la maille de reporting IFRS 17 de certaines grandeurs évaluées à un niveau agrégé .

Evaluation des contrats d'assurance : le modèle général et ses deux adaptations

La norme repose sur une évaluation des passifs à leur valeur d'exécution ou fulfilment value selon une approche par bloc ou building block approach fondée sur une vision prospective reposant sur de estimations plus que sur des éléments historiques observables.

IFRS 17 préconise trois approches pour évaluer le passif d'assurance : un modèle général, un modèle dérivé du modèle général et un modèle simplifié.

Modèle Général : Building Blocks Approach BBA

Ce modèle décompose les passifs d'assurance lors de la 1ère évaluation en blocs :

Bloc 1 : «The fulfilment cash flows» (current estimate):

Il s'agit de la meilleure estimation des engagements techniques (souvent admis comme Best Estimate Liability) ; cette estimation intègre l'ensemble des flux de trésorerie futurs entrants et sortants liés à l'exécution du contrat et attendus par l'assureur : paiements, primes, charges, coûts d'acquisition, etc. et prend en compte l'actualisation.

Bloc 2 : Risk Adjustment :

L'ajustement pour risque est une estimation de l'incertitude existante sur les flux quant à leur montant et leur date d'occurrence. Cet ajustement pour risque représente ainsi la compensation que demanderait un acteur de marché pour couvrir l'incertitude existante liées aux flux. Les assureurs doivent divulguer le niveau de confiance équivalent au RA ce qui implique d'avoir une estimation de la distribution du current estimate.

Bloc 3 : Marge de Service Contractuelle Contractual Service Margin CSM

La CSM représente la part revenant à l'assureur des profits futurs actualisés, non acquis du portefeuille de contrats. Cette marge est constatée à la souscription pour éliminer les profits dégagés lorsque les flux futurs entrants ajustés au risque dépassent les flux futurs entrants ajustés au risque. Cette marge est amortie sur la période de couverture du contrat et est réévaluée à chaque clôture. Toutefois si le groupe de contrats est déficitaire à l'origine, la perte est constatée immédiatement au résultat (P&L) et ne peut être amortie sur les périodes futures.

L'on se trouve alors face aux problématiques de calcul de la CSM par cohorte. Or, dans certains cas, les mécanismes de participation reposent sur des calculs consolidés effectués sur l'ensemble des générations de souscription des portefeuilles considérés. La profitabilité d'une cohorte dépend donc de celle des autres cohortes et il apparaît très délicat en pratique d'évaluer mécaniquement une CSM à l'échelle d'une cohorte marginale.

La norme IFRS 17 exige que les hypothèses retenues pour l'évaluation des «fulfilment cash flows» doivent être mises à jour à chaque date de reporting, elle suppose l'actualisation des flux de trésorerie futurs en ramenant l'ensemble des flux financiers à une même date pour refléter la valeur temps de l'argent. Le taux d'actualisation retenu doit être compatible avec les caractéristiques du passif en termes de duration, de devise et de liquidité.

Le taux d'actualisation est calculé à partir de la courbe des taux en vigueur à la date d'arrêté qui est déterminé par construction à partir du taux sans risque auquel s'ajoute une prime d'illiquidité du passif.

Modèle dérivé du modèle général : Variable Fee Approach VFA

Il s'agit du modèle adapté du modèle général et est réservé pour la comptabilisation de contrats avec participation aux bénéfices directe «insurance contracts with direct participation features», pour lesquels les flux de trésorerie varient en fonction de la performance d'éléments sous-jacents, cas des contrats épargne-retraite avec PB.

Pour ces contrats, les assurés sont propriétaires des éléments sous-jacents que l'assureur les gèrent à leurs profits et non pour son propre compte. La «variable fee» est la part des bénéfices des éléments sous-jacents selon la règle de partage assureur/assuré. Les critères de regroupements des contrats exigés pour le modèle général s'appliquent au modèle dérivé.

Modèle Preminum Allocation approach (PAA), modèle optionnel, avec une approche la plus simplifiée et valable pour les contrats d'une durée de couverture de moins d'un an. Cette approche prévoit au titre des sinistres non survenus de comptabiliser le passif d'assurance par une provision pour primes non acquises.

Pour les sinistres survenus, il y a lieu d'appliquer les principes du modèle général (BBA).

La norme IFRS 17 modifiera ainsi en profondeur la comptabilisation des contrats d'assurance et la présentation du compte de résultat. Son intégration nécessitera de lourdes adaptations particulièrement des systèmes d'informations et une refonte des modèles actuariels de projection des sinistres.

Ceci implique pour les compagnies d'assurance et de réassurance une charge de travail et des coûts très importants liés à l'acquisition ou le développement en interne de nouvelles solutions informatiques, la formation et l'encadrement et l'adaptation des processus opérationnels.

A l'échelle internationale, la plupart des acteurs ont réalisé une phase de cadrage visant à appréhender les impacts d'IFRS 17 sur les données, processus et systèmes et à identifier les principaux écarts entre leur organisation actuelle et une vision de ce que devrait être la cible. Le passage au cours des prochains mois à la phase d'implémentation avec l'établissement d'un plan détaillé traduisant la vision, les principes et les exigences retenues se heurte toutefois aux interrogations existantes sur des sujets structurants.

Les assureurs tunisiens face aux nouveaux enjeux règlementaires : Etat des lieux

Dans l'objectif de suivre le rythme d'évolution des standards internationaux et franchir un grand pas vers la modernisation de l'économie tunisienne, les autorités de régulation en Tunisie ont lancé plusieurs projets de changements de normes comptables et prudentielles.

Les normes Internationales IFRS

Les normes IFRS, référentiel comptable homogène et universel mis en place par L'IASB International Accounting Standards Board ont introduit une révolution de l'information financière avec le principe de la prééminence de la substance sur l'apparence. Ce référentiel implique que le traitement comptable des opérations découle d'une analyse économique des transactions, par opposition à l'analyse juridique pratiquée jusqu'alors dans plusieurs pays.

Ce référentiel comptable constitue une opportunité d'optimisation des processus financiers, de la production des comptes au pilotage de la performance et à la communication financière externe et interne.

Le «corpus IFRS» est composé d'une cinquantaine de normes définies réparties en Normes «sectorielles» comme celles relatives aux contrats d'assurance ou à l'industrie extractive ; Normes «de consolidation» (IAS 7, 27, 28, IFRS 3, 10, 11 et 12 par exemple) définissant les règles en matière d'établissement des états financiers consolidés et de regroupements d'entreprise ; et Normes «opérationnelles» (IAS 16, 17, 36, 38, 37, 19, 32, 39, IFRS 7 par exemple) précisant le cadre d'évaluation et de comptabilisation des actifs et passifs financiers et non financiers, courants et non courants.

Le Conseil National de la Comptabilité a décidé lors de son assemblée générale du 6 septembre 2018 que les sociétés cotées à la bourse des valeurs mobilières de Tunis, aux banques et aux établissements financiers, aux sociétés d'assurance et de réassurance sont appelées à établir leurs états financiers consolidés selon les normes internationales d'information financière (IFRS) à partir du 1er janvier 2021.

A cet effet, les sociétés et établissements concernés sont appelés à mettre en place un plan d'actions, détaillant les étapes nécessaires pour l'implémentation du nouveau référentiel comptable qui sera adopté. Ce plan doit être approuvé par le conseil d'administration ou le conseil de surveillance de l'institution, qui sera assisté par le comité permanent d'audit.

Chaque institution concernée, doit veiller à la constitution d'un comité ou d'un groupe de travail pour le suivi et la supervision de l'exécution dudit plan. Ledit comité rend compte de ses travaux directement au conseil d'administration ou au conseil de surveillance et doit inclure au minimum des responsables des unités chargées du système d'information, du service comptable et financier, du service audit interne et des représentants des sociétés du groupe.

Ce comité sera chargé notamment de :

- Mettre en place le plan d'actions ci-dessus indiqué et l'échéancier d'exécution dudit plan ;

- Recenser les difficultés d'application du nouveau référentiel et les divergences avec le référentiel existant ;

- Préparer une étude d'impact traduisant l'effet de l'adoption des normes IFRS sur la situation financière du groupe.

Cette décision a été suivie par des circulaires émies par la Banque Centrale de Tunisie, le Conseil de Marché Financier et le Comité Général des Assurances imposant aux Entités à Intérêts Publics de préparer une feuille de route et un plan d'action stratégique d'adoption des normes IFRS à partir de janvier 2021.

Dans la foulée, le Comité Général des Assurances a émis la décision n° 1/2020 du 19 juin 2020 relative aux travaux préparatifs pour l'adoption des normes comptables internationales « IFRS/IAS». Cette décision fournit un cadre général de démarche à adopter par les compagnies d'assurances et de réassurance pour encadrer le processus de préparation du passage vers les normes comptables internationales «IFRS/IAS» et à définir une feuille de route pour le projet d'adoption de ces normes.

Parmi les obligations qui incombent aux sociétés d'assurance et de réassurance :

- Soumettre au CGA, le Plan d'Action Stratégique approuvé par leurs Conseils d'administration ou leurs conseils de Surveillance.

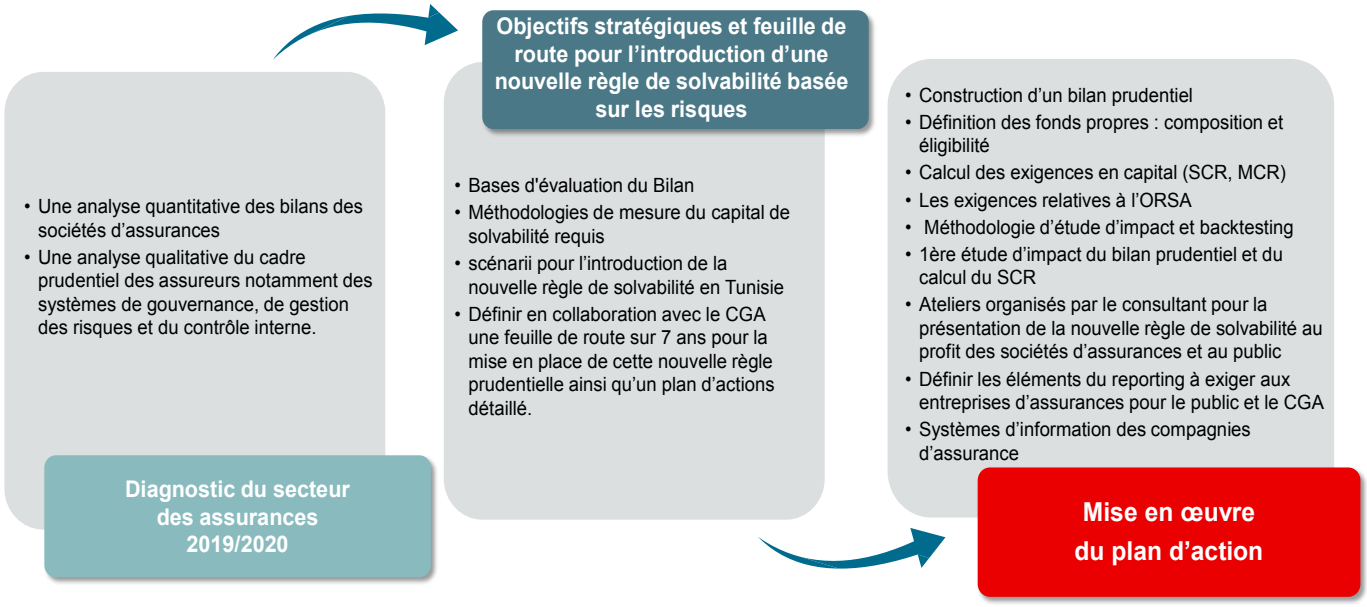
- Soumettre au CGA, dans un délai ne dépassant pas le mois de décembre 2020, une étude d'impact, approuvée par le Conseil d'administration, de l'adoption des normes comptables internationales sur les comptes annuels de la société et ceux du groupe de l'année 2019.

Pour les compagnies d'assurances tunisiennes, le processus de transition aux normes IFRS doit être géré en deux phases. Une première phase consacrée à l'adoption des normes IFRS en vigueur au 1er janvier 2021 notamment en tenant en compte de la norme IFRS 4, Contrats d'assurance, et implémenter dans une deuxième phase la nouvelle norme IFRS 17 qui remplacera la norme IFRS 4 en vigueur jusqu'au 1er janvier 2023. Un exercice transitoire est à prévoir dès 2022 pour la construction du bilan d'ouverture.

Les enjeux d'implémentation des normes IFRS pour le secteur des assurances en Tunisie sont de taille et requièrent de mettre en place une stratégie de transition qui englobe les composantes Système d'information qui est au cœur du projet IFRS, une composante financière liée au coût de la transition, une composante ressources humaines qui nécessite le recours à certaines compétences et enfin une composante opérationnelle impliquée surtout par IFRS 17.

La Solvabilité Basée sur les Risques : un chantier qui vient de démarrer

Un autre chantier non moins important est sur les rails en l'occurrence le projet de la Solvabilité basée sur les risques SBR initié par le régulateur tunisien des organismes d'assurances et de réassurance le CGA. Ce projet s'articule sur les points ci-après et est prévu pour une période de concrétisation de 7 ans.



Le cas du Maroc : Etat des lieux

Les projets règlementaires avancent d'une manière notable

Le processus de convergence des normes comptables avec les référentiels internationaux (IFRS International Financial Reporting Standards) entamé en 2007 s'est limité aux groupes du secteur financier et aux sociétés cotées. En effet, l'ouverture sur les normes IFRS de la comptabilité marocaine s'est faite dès 2007 à travers l'obligation faite aux établissements de crédit de publier leurs états financiers consolidés en normes internationales à partir de 2008 et l'option permise aux entreprises non financières privées et publiques d'utiliser le nouveau référentiel comme base de consolidation à compter de 2007.

Le marché marocain des assurances deuxième en Afrique et 3ème dans le monde arabe se prépare à grands pas pour la transition aux normes IFRS ainsi qu'à un nouveau cadre prudentiel de la solvabilité. L'Autorité de Contrôle des Assurances et de la Prévoyance Sociale (ACAPS) a accéléré la mise en conformité de la supervision du secteur des assurances avec les normes internationales, des études d'impact de l'implémentation de IFRS 17 seront réalisés pour permettre d'ajuster les délais de transition et de lisser les effets sur les résultats et les fonds propres des compagnies d'assurance.

Projet SBR au Maroc

Ce projet de circulaire vise à réviser les règles de solvabilité auxquelles sont soumises les Entreprises d'Assurances et de Réassurance en intégrant l'ensemble des risques encourus par ces entreprises, le cadre prudentiel en vigueur ne prenant en compte que le risque de souscription. A l'instar de la directive européenne «Solvabilité II», ce nouveau cadre prudentiel s'articule autour de 3 piliers:

Le pilier I regroupe les exigences quantitatives, à savoir les règles de valorisation des actifs et des passifs ainsi que les exigences de capital et leur mode de calcul;

Le pilier II porte sur les exigences qualitatives et définit les règles de gouvernance et de gestion des risques, en l'occurrence l'évaluation interne des risques de la solvabilité;

Le pilier III concerne, quant à lui, les obligations de reporting à l'Autorité et de diffusion de l'information au public.

Le secteur continue de dégager une marge de solvabilité largement supérieure au minimum réglementaire exigé. Ne couvrant que le risque de souscription, ces excédents de marge devraient s'inscrire à la baisse avec le passage vers un régime prudentiel de solvabilité basée sur les risques.

Enfin, les exercices de stress tests réalisés en mars 2020 ont fait ressortir à cette date la résilience.

Conclusion

L'exposition aux risques émergents continuera à évoluer durant l'année 2021 et nous assisterons aux mêmes défis qui se sont posés en 2020, notamment en raison de la propagation continue du coronavirus dans de nombreuses régions du monde, de certains changements politiques dans quelques régions et l'aggravation des conditions climatiques dans d'autres.

Cependant, les perspectives du secteur de l'assurance pour 2021 comporteront également quelques problèmes émergents notables qui ne manqueront pas d'impacter l'activité des assureurs et réassureurs. En effet, aux risques majeurs évoqués ci-dessus, nous pouvons ajouter l'émergence importante des risques technologiques, l'interruption d'activité sans dommages, les réformes réglementaires et l'augmentation des sanctions réglementaires, le risque de non-conformité, les changements des normes comptables et prudentielles, la croissance des inégalités et tensions sociales, la dégradation de l'environnement économique et financier…

Jusqu'à présent, de nombreuses leçons tirées de la pandémie de coronavirus ont été tirées. Cependant, peu de modèles de risque prenaient en compte ce type d'événement. Désormais, les professionnels du risque et de l'assurance sont de plus en plus désireux de mieux comprendre les impacts de tels événements, dont nous avons déjà reçu de nombreux avertissements, tels que le risque d'une cyber-attaque massive entraînant une panne mondiale et des pertes financières spectaculaires.

Par ailleurs, le monde de l'assurance et de la réassurance connait de nombreux changements règlementaires et comptables ces dernières années imposés par la nature elle-même de l'activité du secteur de l'assurance qui touche à tous les domaines (Industrie, Services, Commerce, Agriculture…). Ainsi, les assureurs et réassureurs sont appelés à s'adapter à tous les changements et circonstances qui peuvent impacter leur activité et notamment l'activité de leurs clients surtout avec l'émergence continue de nouveaux risques.

Finalement, il est certain que les risques émergents préoccupent les professionnels de l'assurance et la réassurance dans le monde et nécessitent des efforts de compréhension et d'adoption de solutions appropriées à ces risques. Cependant, ils doivent être considérés comme une opportunité et une nouvelle niche de développement de leur activité leur permettant la conquête de nouveaux marchés.

Comité de Rédaction

Tunis Re
Société Tunisienne de Réassurance

2, Avenue du Japon Montplaisir - B.P 29 - 1073 Tunis
Tél. : (216) 71 904 911- Fax: (216) 71 904 930
E-mail : tunisre@tunisre.com.tn
www.tunisre.com.tn
: www.facebook.com/Tunis-Re-178608322175326/
: www.linkedin.com/company/tunis-re/