LUmière sur la CYberassurance

édition 2021

AMRAE

L'AMRAE publie la première étude exhaustive sur la couverture assurantielle du risque cyber en France

L'Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE) publie la première étude objective et exhaustive sur le risque cyber et sa couverture assurantielle.

L'enquête LUCY (LUmière sur la CYberassurance) est une première mondiale : elle doit permettre aux assureurs, courtiers, et assurés, de nouer un dialogue constructif au service d'une meilleure protection de notre tissu économique.

Une étude pilotée par Philippe Cotelle, administrateur et président de la commission Systèmes d'Information de l'AMRAE, vice-président de FERMA et Risk Manager d'Airbus Defence & Space.

L'**AMRAE** (**A**ssociation pour le **M**anagement des **R**isques et des **A**ssurances de l'**E**ntreprise) est l'association professionnelle de référence des métiers du risque et des assurances en entreprise. Elle rassemble plus de 1 500 membres appartenant à plus de 750 organisations privées ou publiques.

L'AMRAE soutient ces organisations dans l'atteinte de leurs objectifs stratégiques et opérationnels pour leur permettre d'améliorer leurs performances et de maîtriser leurs risques.

La gestion des risques est une démarche vertueuse protégeant l'entreprise, ses employés et partenaires, y compris assureurs et, partant, l'économie dans sa globalité.

AMRAE l'Association rassemble les acteurs majeurs des lignes de maîtrise du risque (Risk Management, contrôle et audit internes, assurance, juridique, éthique…).

A travers ses comités scientifiques, ses publications et ses nombreuses manifestations, l'AMRAE produit pour ces experts les contenus qui nourrissent leurs compétences, leur évolution dans leur métier et leur contribution à la réussite de la stratégie de l'entreprise.

Avec AMRAE Formation, elle répond à leurs besoins de développement professionnel adapté aux évolutions des organisations, en dispensant des formations certifiantes de haut niveau.

AMRAE Les Rencontres organise le congrès annuel de référence des métiers du risque et des assurances (plus de 3 000 congressistes en 2020). Ces trois jours constituent le rendez-vous métier incontournable des acteurs de la maitrise des risques et de son financement.

Ensemble,
mieux comprendre pour mieux protéger

Dans une économie qui se digitalise à marche forcée, le risque cyber est encore mal compris. Les entreprises et les collectivités publiques n'ont pas pris la mesure du danger alors que les pirates gagnent en expertise.

Parallèlement, l'industrie de l'assurance peine à trouver l'équilibre économique des garanties cyber : après une course à la souscription, les assureurs marquent le pas devant l'ampleur du risque à couvrir.

Pour juguler la menace, les assureurs comme les assurés doivent monter en maturité : les entreprises et les collectivités publiques doivent améliorer la prévention et la protection de leurs systèmes d'information. Quant au marché de l'assurance, il doit devenir plus clair et plus lisible.

En mettant des chiffres sur les niveaux de couverture assurantielle et de sinistralité des entreprises et des collectivités publiques, l'étude LUCY contribue à la maturation du marché.

L'assurance cyber n'a pas encore trouvé son équilibre : avec un taux de couverture des entreprises et un volume de primes encore trop limités, les assureurs ne parviennent pas à trouver les conditions de la mutualisation indispensable au règlement des sinistres de forte intensité.

Ce manque de maturité n'explique pas tout : le marché américain est, certes, un peu plus mûr ; mais les taux de primes cyber sont en augmentation constante. Mieux vaut donc se préparer à des tensions inflationnistes sur le marché européen.

Une bonne connaissance du risque cyber permettra de maîtriser ces tensions. C'est toute l'ambition de l'étude LUCY : l'AMRAE l'a précisément menée pour poser les bases d'un dialogue constructif entre les assureurs, les assurés et les courtiers.

Les entreprises et les collectivités publiques ont besoin de garanties réellement protectrices et sur-mesure, à des tarifs adaptés et lissés dans le temps. Dans une conjoncture déjà difficile, elles ne peuvent pas prendre le risque de voir leur prime exploser au moindre sinistre.

Pour les assureurs, l'équilibre technique et financier du risque cyber repose à la fois sur une meilleure mutualisation et sur le développement des stratégies de prévention dans les entreprises et les collectivités publiques.

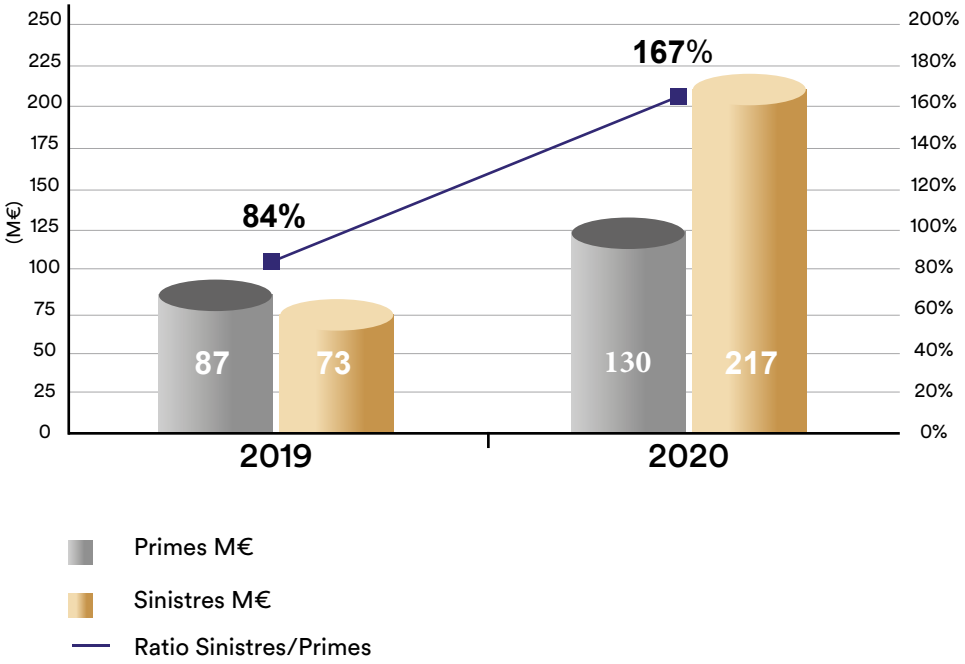
Les courtiers spécialistes du risque d'entreprises et les Risk Managers ont un rôle clé à jouer dans la montée en maturité du marché de l'assurance cyber. Ils ont travaillé ensemble pour mener la première étude sur ce thème et je m'en félicite.

Oliver Wild,
Président de l'AMRAE

LUmière
sur la CYberassurance

Une sinistralité globale en forte augmentation, expliquée par 4 sinistres de forte intensité

Menée en partenariat avec huit des grands courtiers spécialistes du risque d'entreprise, LUCY fait apparaître une **augmentation du volume de primes de 49 %**, qui est passé de 87 M€ en 2019 à 130 M€ en 2020. Mais **cette croissance est très inférieure à celle du montant des indemnisations versées** qui a été multiplié par 3, passant de 73 M€ en 2019 à 217 M€ en 2020. Pour les assureurs, le ratio Sinistres sur Primes (S/P) est donc passé de 84 % à 167 %.



Ces données permettent de mieux comprendre les **tensions en cours sur le marché de l'assurance** cyber. Les entreprises se voient actuellement proposer des réductions de garanties pour des tarifs plus élevés. Sans doute à juste titre dans certains cas, mais certainement pas dans tous les cas. Car si l'on se penche de plus près sur ces résultats techniques, on observe plusieurs facteurs explicatifs :

- Le volume d'indemnisation de sinistres a, certes, été multiplié par 3 entre 2019 et 2020. Mais **cette inflation n'est due qu'à 4 sinistres de très haute intensité** (entre 10 et 40 M€ d'indemnisation chacun) déclarés par des grandes entreprises. Sans ces 4 sinistres, qui ne représentent que 1 % des sinistres indemnisés en 2020, les résultats techniques de l'ensemble de la ligne cyber auraient été identiques à ceux de 2019.
- **87 % des grandes entreprises sont couvertes par un contrat d'assurance cyber, mais pour une couverture trop limitée (38 M€ en moyenne)** au regard de leur exposition. Elles ont besoin que l'offre d'assurance se développe pour augmenter leurs capacités. Mais les assureurs resteront réticents tant que le volume global de primes ne leur permettra pas de faire face aux sinistres de haute intensité. Il faut donc que la demande augmente pour que l'offre soit suffisante. Ou que l'offre soit suffisante pour susciter la demande… Il y a urgence à sortir de ce **cercle vicieux** : les **grandes entreprises représentent 82 % du volume de primes** sur le marché de l'assurance cyber.
- **Sous assurance des ETI et des collectivités publiques :** les Entreprises de Taille Intermédiaire (ETI) et les PME ne connaissent pas ce problème d'offre : **seulement 8 % des ETI sont assurées pour une couverture moyenne de 8 M€**. Une telle capacité est facilement accessible sur le marché, à des taux de primes très attractifs. Sur ce marché, le véritable enjeu est de **sensibiliser les entreprises au risque cyber, qui est réel** : en 2019, les indemnisations versées aux ETI et aux PME ont représenté plus de 40 M€. Il existe trois moyens complémentaires de se protéger : la prévention, la gestion de crise et l'assurance. Le défaut de protection actuel est une **menace pour l'économie française.**
- Les **collectivités publiques** sont, elles aussi, très largement sous-assurées alors que leur **exposition est réelle,** comme les nombreuses attaques enregistrées depuis le début de l'année le montrent.

LES RECOMMANDATIONS DE L'AMRAE

- La politique de gestion des risques de l'organisation, privée comme publique, est la priorité. Prendre conscience de sa dépendance au numérique et donc de son exposition, la mesurer, développer une politique de prévention et de transfert du risque résiduel par une stratégie d'assurance efficace est absolument indispensable pour toutes les entreprises privées ou publiques, quelles que soient leur taille et leur activité.

- Développer une offre d'assurance qui réponde aux besoins des grandes entreprises et accéder à la mutualisation qui permettra de faire face aux sinistres de très haute intensité et rendra les résultats techniques moins volatils.

- Sensibiliser les ETI, les PME, les TPE et les collectivités publiques à la réalité du risque cyber et les inciter à déployer une politique de gestion du risque cyber qui intègre l'assurance.

- Ne pas commencer par l'assurance : ce n'est qu'une composante - certes indispensable - de la gestion des risques. Prendre conscience de son exposition au risque cyber, identifier les risques et déployer des mécanismes de prévention permet de ne transférer que les risques résiduels à l'assureur.

CHIFFRES CLÉS 2020

87 %
des grandes entreprises
mais seulement
8 %
des entreprises de taille intermédiaire ont **souscrit une assurance cyber.**

38 M€
hauteur moyenne de la **couverture des grandes entreprises.**

X 3 : **augmentation de la sinistralité**

surtout en intensité : le montant global des indemnisations a été multiplié par 3, passant de 73 M€ en 2019 à 217 M€ en 2020.

+ 19 %
pour les grandes entreprises et
+ 28 % pour les ETI :
augmentation des taux de primes entre 2019 et 2020.

167 % vs 84 %
ratio Sinistres/Primes de 2020 vs celui de 2019.

Cette **dégradation du ratio S/P** est presque **exclusivement liée à la survenue de quatre sinistres importants,** indemnisés entre 10 et 40 M€ chacun. Sans ces 4 sinistres, les résultats techniques auraient été **stables.**

Le risque cyber, cet inconnu…

Durant l'année 2020, le Parquet de Paris a été saisi à 397 reprises pour des affaires de « rançongiciels », ces logiciels malveillants qui paralysent le système d'information des entreprises si ces dernières ne s'acquittent pas d'une rançon. On peut s'attendre au doublement de ce chiffre en 2021.

Toutes les activités sont touchées. Durant les quatre premiers mois de l'année 2021, le « Mag IT[1] » a recensé et documenté pas moins de 80 attaques visant des acteurs de la santé (une dizaine d'hôpitaux et cliniques, le groupe pharmaceutique Pierre Fabre, la Mutuelle nationale des hospitaliers), des collectivités territoriales (les villes d'Angers, Douai, Houilles, Pontault-Combault, Elancourt, la communauté de communes de l'Est lyonnais, le département de la Vienne), des groupes industriels (Trigano, Bénéteau, Lactalis, Mersen) ou immobiliers (Coffim, 1001 vies Habitat, Servimo), des activités de services (Ucar, Wonderbox, In Extenso)… et même Coallia, un acteur associatif du logement social pour les plus démunis.

> *Le manque de données robustes sur le taux de couverture des entreprises et sur leur sinistralité est un frein au développement de l'assurance cyber.*

Le coût de ces sinistres reste difficile à évaluer. Il est parfois marginal. Mais il peut aussi se chiffrer en centaines de millions d'euros : 220 M€ de pertes pour le groupe Saint-Gobain en 2017, 70 M€ pour Eurofins en 2019, et 50 M€ pour le groupe Sopra Steria en 2020… Une perte sèche pour certains, car ces dommages n'étaient pas tous couverts par une police d'assurance.

1 https://www.lemagit.fr/essentialguide/Contre-les-ransomwares-combiner-preparation-prevention-et-detection

Le risque cyber reste tabou : l'ampleur, le coût réel et le niveau d'indemnisation de ces sinistres sont rarement rendus publics. Si bien que les chiffres et les données régulièrement brandis pour alerter les entreprises sur l'importance de ce risque relèvent davantage de l'extrapolation, de la spéculation ou du sondage que de la véritable enquête statistique. Ce manque de données est un frein au développement du marché de l'assurance cyber.

Toutes les organisations - entreprises, collectivités publiques ou associations- ont deux grands moyens de se protéger contre ce risque. En amont, elles peuvent prévenir les attaques : en sécurisant leurs systèmes d'information, en identifiant leurs vulnérabilités, en formant leurs équipes aux enjeux de la sécurité et aux techniques des pirates… L'humain reste en effet le maillon faible de la sécurité : la moitié des attaques découlent d'erreurs humaines. En aval, l'assurance permet de financer la gestion de crise avec des experts en cyber assistance, les frais de notification en cas de perte des données, ainsi que tous les dommages financiers liés directement ou indirectement à l'attaque : pertes d'exploitation, frais d'experts informatiques, frais d'avocats, communication de crise et, comme on a pu le découvrir récemment, paiement d'une rançon[2].

> *87 % des grandes entreprises et*
> *8 % des entreprises de taille intermédiaire*
> *ont souscrit une assurance cyber*

Les assureurs considèrent depuis des années déjà que le risque cyber est un marché-clé et un relais de croissance. Mais cette nouvelle ligne peine encore à décoller : l'étude conduite par l'AMRAE révèle que si 87 % des grandes entreprises françaises sont effectivement couvertes, moins de 8 % des entreprises de taille intermédiaire (ETI) ont souscrit une assurance contre le risque cyber.

Cette sous-couverture fait courir des risques aux entreprises et aux collectivités publiques concernées, mais aussi à l'ensemble de leur écosystème : sous-traitants, fournisseurs, clients, partenaires commerciaux…

2 https://www.lesechos.fr/tech-medias/hightech/rancongiciels-les-entreprises-accusees-de-payer-trop-facilement-les-rancons-1307890

C'est aussi un frein au développement de l'assurance cyber : faute de mutualisation, avec un historique de données disponibles limité, les assureurs peinent à trouver un modèle économique viable pour ces garanties.

On comprend mieux pourquoi le renouvellement des polices cyber est particulièrement tendu depuis un an. Alertés par les augmentations de taux, le relèvement des niveaux de franchise et la baisse des capacités qui leur sont proposés, les Risk Managers ont besoin d'y voir plus clair.

L'AMRAE a donc mené une grande enquête auprès des acteurs-clés de la couverture assurantielle : les courtiers spécialisés en risques d'entreprises et des collectivités publiques (voir méthodologie page 13). Une analyse de leur portefeuille permet d'avoir une vision à la fois objective et exhaustive de ce risque encore méconnu et mal compris.

Cette étude - une première mondiale - va nourrir le dialogue entre les assureurs, les courtiers et les entreprises et collectivités publiques.

Il est en effet essentiel de créer une référence commune à toutes les parties prenantes pour permettre un développement sécurisé et pérenne de l'assurance cyber, nécessaire pour protéger les entreprises, les collectivités publiques et le tissu économique de nos territoires.

Une vision internationale de l'assurance des grandes entreprises

Quand elles souscrivent une police cyber, les grandes entreprises françaises font largement appel au marché international : leurs risques sont placés auprès de plusieurs assureurs (parfois plus de 20) dans le monde entier. En interrogeant les courtiers qui sont précisément chargés de placer ces risques, l'étude LUCY permet d'avoir une vision globale de l'assurance cyber des entreprises françaises, qui va bien au-delà des contrats souscrits auprès des assureurs français.

Une étude exhaustive du risque cyber

Un état des lieux du marché de l'assurance cyber est nécessaire pour créer les conditions d'un dialogue constructif avec les assureurs. L'Association pour le management des risques et des assurances de l'entreprise l'a voulu aussi objectif et exhaustif que possible pour répondre aux questions suivantes : combien d'entreprises souscrivent une police cyber ? Avec quel niveau de primes et quelles capacités ? Pour quelle sinistralité et quels résultats techniques ?

L'AMRAE aurait pu interroger ses 1 500 membres travaillant dans 750 entreprises et collectivités publiques : cette étude aurait été sans doute plus robuste et complète que la plupart des données circulant actuellement sur le marché. Mais pour être véritablement représentatif, un tel sondage aurait dû être élargi à plusieurs milliers d'entreprises.

De même, les données produites par la Fédération française de l'assurance (FFA) ne sont qu'un reflet partiel du marché : la FFA recueille les données de tous les assureurs français. Mais les polices cyber des entreprises, notamment celles des grands groupes, sont généralement souscrites auprès de plusieurs assureurs qui ne sont pas tous présents en France.

Pragmatique, l'AMRAE s'est tournée vers les intermédiaires indispensables entre les assureurs et les entreprises : les courtiers spécialistes des risques d'entreprise. *« C'est le meilleur observatoire pour avoir une vision réelle et exhaustive du marché*, explique Philippe Cotelle, président de la commission Systèmes d'information de l'AMRAE. *C'était aussi le seul moyen de garantir l'anonymat des réponses.* » Sur un sujet aussi sensible que le risque cyber, la confidentialité a été une exigence absolue de l'AMRAE : les réponses transmises par les courtiers ont été anonymisées en amont, de sorte qu'aucune entreprise ne peut être reconnue. Puis, les réponses transmises par chaque courtier ont été anonymisées avant agrégation par l'équipe projet.

Les principaux courtiers spécialistes du risque d'entreprise - à l'exception d'un seul - ainsi que Planète CSCA (l'organisation professionnelle du courtage) ont participé à cette étude. Ce qui permet d'avoir un reflet fidèle du marché de l'assurance cyber des grandes entreprises, des entreprises de taille intermédiaire (ETI) et, dans une moindre mesure, des PME, des TPE et des collectivités publiques.

Méthodologie

- L'étude LUCY est basée sur une enquête menée entre le 21 janvier et le 19 février 2021 auprès des courtiers spécialistes du risque d'entreprise.
- Le questionnaire a été conçu de façon collaborative avec les courtiers et comprend deux grands volets : le niveau de couverture des entreprises et des collectivités publiques (nombre d'entreprises ayant souscrit une police cyber, couverture souscrite, montant de la prime brute) et les sinistres indemnisés (nombre de sinistres, élément déclencheur, nature de l'impact, montant de l'indemnisation).
- Pour respecter la confidentialité absolue des assurés, les courtiers n'ont transmis que des données consolidées à l'échelle de leur portefeuille. Ces données ont ensuite été consolidées par l'équipe projet de l'AMRAE pour construire une vision à l'échelle du marché français. Les données soumises par chaque courtier ont ensuite été détruites.
- Ces résultats ont été ventilés par typologie d'assurés, selon la nomenclature Insee pour les entreprises : grandes entreprises (plus d'1,5 Md€ de CA), ETI (entre 50 M€ et 1,5 Md€ de CA), PME (entre 10 et 50 M€ de CA), TPE (moins de 10 M€ de CA) ; et, pour les collectivités publiques, par régions, métropoles, communes de plus de 5 000 habitants-intercommunalités, communes de moins de 5 000 habitants.

Une vision partagée

Pour bien comprendre les problématiques et améliorer le protocole de l'étude, l'AMRAE, dans sa volonté d'exhaustivité, a pu échanger avec l'ensemble des parties prenantes.

L'Agence nationale de la sécurité des systèmes d'information (Anssi) : créée en 2009, cette autorité nationale est un acteur majeur de la cybersécurité. Elle apporte son expertise et son assistance technique aux entreprises et aux administrations, avec une mission renforcée au profit des Opérateurs d'Importance Vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques. Elle a donc une excellente connaissance des attaques, de leur nombre et de leur mode opératoire. Mais elle manque encore de données sur leur impact financier :

avoir une meilleure vision du coût de ces attaques va lui permettre de mieux sensibiliser les entreprises et les administrations à l'importance du risque cyber.

L'institut des actuaires : cette organisation regroupe 4 500 professionnels de la modélisation mathématique. Depuis sa création, au milieu du XIXe siècle, elle poursuit trois missions : veiller à l'excellence de l'actuariat (en établissant notamment des normes professionnelles et des règles déontologiques), encourager la recherche et se mettre au service de l'intérêt général. C'est à ce titre que l'Institut des actuaires s'est associé à cette étude, en participant notamment à l'analyse des données consolidées dans le but de mieux modéliser ce risque complexe.

La Fédération Française d'Assurance (FFA) : elle rassemble 260 sociétés d'assurance et de réassurance représentant 99 % du marché. Elle a pour mission de représenter les intérêts du secteur auprès des pouvoirs publics et des différents partenaires, en France et à l'international. Elle intervient dans le débat public sur des sujets sociétaux. La FFA regroupe également les forces de réflexion et d'analyse des enjeux financiers, techniques et juridiques de la profession. Elle centralise les données statistiques et s'assure que les informations sont diffusées auprès des partenaires et des médias. Elle organise également des actions de prévention et de formation.

Les courtiers spécialistes du risque d'entreprise

Cette étude a été menée auprès de huit grands courtiers spécialistes du risque d'entreprise : AON, Diot, Filhet Allard, Marsh, Siaci saint Honoré, Verlingue, Verspieren, Gras Savoye-Willis Towers Watson.

Planète CSCA, le syndicat du courtage, a également été mis à contribution, notamment pour avoir une meilleure vision du marché des PME.

Une vision fiable et objective

Cette analyse du risque cyber par le prisme des polices rédigées par les courtiers spécialistes des risques d'entreprise permet d'avoir une vision juste, précise et exhaustive du marché des grandes entreprises et des Entreprises de taille intermédiaire : sur le segment des entreprises réalisant plus de 10 M€ de chiffre d'affaires, l'étude donne l'image la plus fiable du marché à date.

Le niveau de fiabilité s'érode à mesure que la taille des entreprises se réduit : entre 2 M€ et 10 M€ de chiffre d'affaires, les résultats restent toutefois très fiables. Ils le sont nettement moins pour les entreprises réalisant moins de 2 M€ de chiffre d'affaires : les courtiers de proximité, les agents généraux et les bancassureurs, qui sont les partenaires privilégiés des TPE et des PME, n'ont pas pu être sollicités dans le cadre de la première édition de cette étude.

Par ailleurs, il reste délicat de parler de tendance avec des données sur les seules années 2019 et 2020 : mieux vaut attendre d'avoir quatre ou cinq ans d'historique pour tirer des conclusions robustes sur l'évolution des taux de primes et des résultats techniques.

Données analysées par l'étude LUCY

1 879 *entreprises et collectivités publiques ont souscrit un contrat d'assurance cyber au cours des années 2019 et 2020.*

328 *sinistres indemnisés en 2019 et 2020.*

Des ambitions internationales

L'AMRAE a lancé cette étude sur l'assurance cyber avec beaucoup d'espoirs et peu de certitudes. Ses premiers résultats la confortent dans l'idée d'en faire un rendez-vous récurrent : l'étude LUCY va être reconduite chaque année en partenariat avec les courtiers pour suivre l'évolution de ce risque dans la durée.

Au regard du caractère international de la plupart des polices d'assurance cyber, l'AMRAE va - comme elle l'a fait pour son panorama des systèmes d'information de gestion des risques - élargir cette enquête à l'ensemble du marché européen, avec le support de ses partenaires européens. En parallèle, l'AMRAE souhaite étendre l'enquête aux marchés américains et asiatiques. En effet, le risque cyber ne connaît pas de frontières et les stratégies des grands assureurs sont établies au niveau mondial.

Le marché américain a une spécificité : le montant colossal des coûts de notification et des frais d'avocats afférents en cas de fuite de données personnelles.

Mieux comprendre les différents marchés de l'assurance cyber, la façon dont les polices sont rédigées, le montant des primes, le niveau des capacités souscrites ainsi que l'évolution de la sinistralité est utile à l'ensemble des parties prenantes : les assureurs, les courtiers et leurs clients (entreprises et collectivités publiques). Car le marché français ne pourra réellement décoller que quand les assureurs auront trouvé les conditions de la mutualisation qui permettent aux assurés de se sentir réellement protégés.

> *« Cette étude va être reconduite chaque année, en partenariat avec les courtiers. Elle sera également élargie au marché européen dans un premier temps, puis à l'échelle mondiale.*

Des entreprises et des collectivités publiques peu et mal couvertes

Des entreprises et des collectivités publiques peu et mal couvertes

L'assurance contre le risque cyber n'a pas encore totalement pénétré le tissu économique français. Le taux de couverture des entreprises et des collectivités publiques reste bas. On peut aussi se demander, au vu des résultats de l'étude LUCY, si les capacités qu'elles souscrivent sont à la mesure de leur exposition au risque cyber.

87% des grandes entreprises sont assurées

Le taux de couverture des entreprises et des collectivités publiques contre le risque cyber restait à ce jour inconnu. L'étude LUCY vient enfin combler cette lacune : 87 % des grandes entreprises sont assurées contre ce risque. En revanche, le Entreprises de taille intermédiaires (ETI), les PME et les collectivités publiques ne recourent à l'assurance cyber que de façon marginale, ce qui suscite de véritables inquiétudes.

Couverture a minima et inadaptée pour les grandes entreprises

Le taux de couverture des grandes entreprises a bondi de 15 points en un an pour atteindre 87 % en 2020. Les 13 % restants (soit 34 grandes entreprises réalisant plus d'1,5 milliard d'euros de chiffre d'affaires sur les 287 recensées par l'Insee) n'ont pas souscrit de police spécifique. Cela ne veut pas dire qu'elles ne sont pas couvertes : elles peuvent avoir choisi de s'auto-assurer par la mise en place d'une captive (c'est-à-dire une filiale jouant le rôle d'un assureur) ; elles peuvent aussi avoir souscrit une police Responsabilité civile (RC) intégrant des garanties cyber. L'étude ne le dit pas.

Elle livre en revanche un indice intéressant sur la stratégie des entreprises qui souscrivent une police cyber : leur niveau de couverture semble très inférieur à leur exposition au risque cyber. La capacité moyenne souscrite par les 87 % de grandes entreprises qui ont fait le choix de s'assurer est restée stable en 2020, autour de 38 M€. Or, les attaques qui ont ciblé de grandes entreprises ces dernières années se sont soldées par des centaines de millions d'euros de pertes qui ne sont pas toujours assurées.

Cela n'a rien d'étonnant : pour une entreprise réalisant plus d'1,5 Md€ de chiffre d'affaires, le coût d'un arrêt total de l'activité pendant un ou plusieurs jours se chiffre en millions d'euros. Auxquels s'ajoutent les coûts de gestion de crise, le risque de réputation, les éventuels frais de notification en cas de pertes de données, etc. On peut donc considérer que les grandes entreprises sont très nettement sous-assurées.

Le coût des sinistres cyber reste difficile à évaluer. Il est parfois marginal. Mais il peut aussi se chiffrer en centaines de millions d'euros : 220 M€ de chiffres d'affaires pour le groupe Saint-Gobain en 2017, 70 M€ pour Eurofins en 2019, et 50 M€ pour le groupe Sopra Steria en 2020… Une perte sèche pour certains, car ces dommages n'étaient pas tous couverts par une police d'assurance.

> *En 2020, les grandes entreprises assurées ont souscrit une capacité moyenne de 40 M€.*

Entreprises de taille intermédiaire : une adoption trop lente, une couverture inadaptée

Le nombre d'Entreprises de taille intermédiaire (ETI) ayant souscrit une assurance contre le risque cyber a bondi de 43,6 % en 2020. Une telle croissance serait encourageante si le taux de couverture des ETI ne restait pas aussi bas : les données recueillies dans le cadre de l'étude LUCY montrent que sur les 5 763 entreprises françaises réalisant entre 50 M€ et 1,5 Md€ de chiffre d'affaires, seulement 441 ont une couverture assurantielle contre le risque cyber[3]. Moins de 8 %.

Ce chiffre est préoccupant : il montre que la conscience du risque cyber et le principe de la protection assurantielle n'ont pas encore pénétré notre économie. Une entreprise dont le chiffre d'affaires flirte avec le milliard d'euros doit avoir une gestion globale du risque cyber, à base de prévention et d'assurance.

De plus, l'étude montre que les ETI qui s'assurent sont - tout comme les grandes entreprises - encore sous-protégées. La capacité moyenne souscrite sur ce segment n'est que de 8 M€ : un niveau probablement très inférieur à leur exposition réelle au risque cyber, comme on a pu le voir au cours de l'année 2020 (voir page 26).

> *Pour une ETI ou une PME, s'assurer contre le risque cyber devrait être aussi naturel que se couvrir contre l'incendie ou les catastrophes naturelles.*

3 https://www.lemagit.fr/essentialguide/Contre-les-ransomwares-combiner-preparation-prevention-et-detection

Les PME ignorent les assurances cyber

En 2020, seulement 362 des 140 000 PME réalisant entre 10 et 15 M€ de chiffre d'affaires ont souscrit une assurance cyber auprès de leur courtier. Ce chiffre est sans doute sous-estimé car elles peuvent aussi souscrire ce type de garanties auprès d'un agent général d'assurance, ou d'un courtier de proximité autre que ceux répondant à l'étude. Mais il a le mérite de dessiner une tendance : le taux de couverture des PME a certes progressé de 16,3 % entre 2019 et 2020. Mais il reste trop faible au regard de l'impact potentiel du risque cyber sur une chaîne de valeur. Il faut aller jusqu'au troisième chiffre après la virgule pour mesurer leur taux de couverture actuel : 0,0026 %.

Des collectivités publiques toujours sous-équipées

Depuis le début de l'année, les collectivités territoriales françaises ont été particulièrement visées : une dizaine de villes (Angers, Douai, Houilles, Pontault-Combault, Elancourt…), la communauté de communes de l'Est lyonnais, le département de la Vienne ont été touchés par une cyberattaque. Leur taux de couverture en assurance cyber est pourtant resté stable en 2020 : autour de 1 %. Mais il tend à s'élever avec la taille de l'organisation : les régions, départements et métropoles sont par exemple plus souvent équipés que les communes.

	Effectif 2020 (selon les catégories de l'Insee)	Nombre de contrats d'assurance cyber en 2019	Nombre de contrats d'assurance cyber en 2020	Croissance 2019/2020	Taux de couverture Cyber 2020
Grandes entreprises (plus d'1,5 Md€ de CA)	287	207	253	+ 22,2 %	87 %
Entreprises de taille intermédiaire (50 M€ à 1,5 Md€ de CA)	5 763	307	441	+ 43,6 %	7,6 %
Petites et moyennes entreprises (10 à 50 M€ de CA)	139 971	311	362	+ 16,3 %	0,0026 %
Régions, départements, métropoles	NC	48	48	0	NC
Communes de plus de 5 000 habitants et intercommunalités	2 204	27	27	0	1 %

Source : Etude LUCY menée par l'Amrae en 2021.

Un volume de prime encore limité

En 2020, le volume global des primes d'assurance versées par des entreprises françaises au titre des garanties contre le risque cyber a représenté 129,6 M€. Il n'était que de 87,2 M€ en 2019, soit une croissance supérieure à 48 %.

Cette croissance est avant tout portée par l'amélioration du taux de couverture puisque le nombre d'entreprises assurées a augmenté de 35 % en moyenne (+22,2 % pour les grands groupes et +43,6 % pour les ETI).

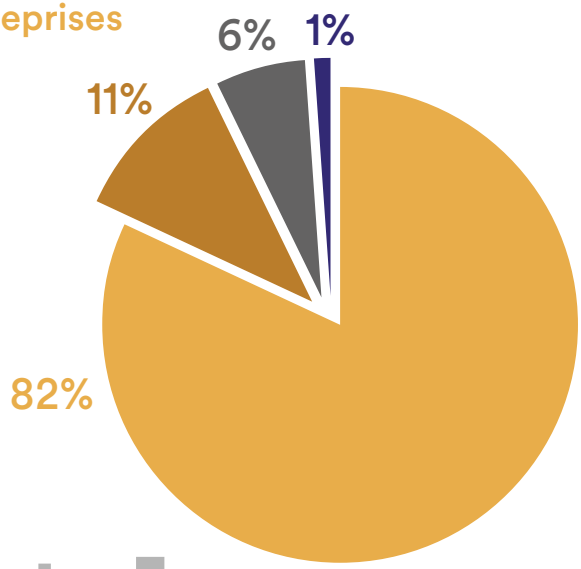
Mais elle doit être relativisée : ces 129,6 M€ sont une goutte d'eau dans l'océan de 8,12 Md€ de cotisations d'assurances des biens professionnels et agricoles[4]. Un tel montant semble aussi très limité au regard de l'exposition cumulée des entreprises : au cours des trois années écoulées, de grandes entreprises ont subi des dommages supérieurs à 50 M€.

> *Le volume de primes perçues par les courtiers ayant participé à l'enquête au titre de l'assurance cyber en 2020 est de 129,6 M€, en hausse de 48 % par rapport à 2019.*

Le marché est porté par les grandes entreprises

Répartition des 129,6 M€ de primes d'assurance payées en 2020 par catégories d'entreprises et de collectivités :

- **Grandes entreprises : 105,9 M€**
- **ETI : 14,9 M€**
- **PME et TPE : 7,6 M€**
- **Collectivités publiques : 1,3 M€**



4 Source : FFA

Des taux de primes en hausse

La croissance du volume de primes d'assurance cyber a également été portée par l'augmentation des taux de prime. C'est l'une des grandes révélations de l'étude LUCY, qui a permis de calculer les taux de primes moyens pratiqués en fonction de la taille des entreprises et de la capacité moyenne souscrite[5]. Ce taux moyen a été obtenu en faisant le rapport entre le volume total de prime et la capacité moyenne souscrite par tous les assurés de la catégorie considérée.

Pour les ETI, le taux de prime moyen est passé de 0,34 % en 2019 à 0,45 % en 2020. L'augmentation peut sembler importante. Mais les ETI continuent à payer leur couverture plus de 2 fois moins cher que les grandes entreprises, dont le taux de prime moyen est passé de 0,93 % en 2019 à 1,03 % en 2020.

Cet écart de 1 à 2 peut s'expliquer : d'une part, le périmètre de risques des ETI est a priori mieux contrôlé que celui des multinationales car il est plus limité. Même si - nous le verrons par la suite - leurs moyens de prévention semblent moins développés. De plus, les grandes entreprises recherchent des capacités plus importantes auprès des assureurs : des niveaux de couverture difficiles à trouver aujourd'hui sur le marché. En revanche, sur le marché des capacités moyennes, l'offre est importante, donc le marché plus concurrentiel.

Ce taux est purement indicatif. En effet nous ne prenons pas en compte les potentielles franchises ou auto assurances qui influenceraient à la hausse le taux réel de prime appliqué. Cependant elles seront plutôt destinées aux grandes entreprises qu'aux ETI et renforceraient d'autant plus l'écart de taux entre les grandes entreprises et les ETI. Etant donné le niveau des franchises faibles appliqué généralement sur le marché en 2019 et 2020, cet indicateur est à notre sens fiable et révélateur d'une tendance exploitable.

> *Le taux de prime moyen des grandes entreprises est plus de 2 fois supérieur à celui des ETI.*

5 Ce calcul ne prend pas en compte les franchises et rétentions qui pourraient être appliquées à certains contrats.

Inflation en vue

En accélérant la transformation digitale de l'économie, la crise sanitaire a fait du risque cyber un enjeu plus essentiel que jamais. Il est indispensable de sensibiliser les entreprises et les collectivités publiques et de les prévenir qu'après une année 2020 à forte sinistralité (voir page 26), les taux de primes ont tendance à augmenter pour les grandes entreprises comme pour les ETI et les PME. Cette inflation pourra toutefois être en partie jugulée par le relèvement des franchises ou, pour les grandes entreprises, par le développement de l'auto-assurance (via la mise en place ou l'utilisation de captives).

Taux de prime : grand écart entre les grandes entreprises et les ETI

Entreprises	Nombre d'entreprises couvertes en 2019	Montant cumulé de prime cyber 2019	Capacité cyber moyenne souscrite en 2019	Taux de prime cyber moyen en 2019	Nombre d'entreprises couvertes en 2020	Montant cumulé de prime cyber en 2020	Capacité souscrite en 2020	Taux de prime cyber moyen en 2020
Grandes entreprises	207	73 118 563 €	38 085 652 €	0,93 %	251	105 891 882 €	41 030 677 €	1,03 %
ETI	307	8 093 921 €	8 138 553 €	0,32 %	441	14 872 640 €	7 567 604 €	0,45 %
PME	311	2 932 394 €	1 934 341 €	0,49 %	362	5 287 862 €	2 066 514 €	0,71 %
TOTAL	**825**	**84 144 878 €**	**13 313 752 €**	**0,77 %**	**1054**	**126 052 384 €**	**13 647 146 €**	**0,88 %**

Source : Etude LUCY menée par l'Amrae en 2021.

Grandes entreprises : des sinistres XXL

En 2019, comme en 2020, les grandes entreprises couvertes par une police cyber ont déclaré 90 sinistres. On peut donc parler de stabilité dans la fréquence, même s'il est difficile de parler de réelle tendance sur seulement deux ans.

En revanche, les sinistres semblent s'être considérablement intensifiés : le montant moyen d'indemnisation a été multiplié par 6, passant de 31,8 M€ en 2019 à 201,5 M€ en 2020.

En réalité, parler de moyenne n'a pas vraiment de sens car le risque cyber est particulièrement volatil : en 2019, aucun sinistre a plus de 10 M€ n'a été déclaré ; l'année suivante, quatre sinistres ont été indemnisés à hauteur de 10 à 40 M€ chacun. Peut-être ont-ils coûté encore plus cher aux entreprises concernées : l'indemnisation étant limitée par la capacité souscrite et le montant de la franchise, l'étude ne permet pas de le savoir précisément.

Ces quatre sinistres ont, à eux seuls, fait plonger les résultats techniques des grandes entreprises en zone rouge écarlate : leur ratio Sinistres/Primes est passé de 44 % en 2019 à 190 % en 2020. Cela signifie que l'an passé, les assureurs ont, sur ce segment d'entreprises, versé près de deux fois plus d'indemnisations qu'ils n'ont perçu de primes.

Grandes entreprises : très forte augmentation des coûts d'indemnisation

	Grandes entreprises	Entreprises de taille intermédiaire	Fréquence des sinistres en 2019	PME - TPE - Public	Total
Indemnisations versées en 2019	31,8 M€	38,9 M€	2,8 M€	73,5 M€	73,5 M€
Indemnisations versées en 2020	201,5 M€	12,7 M€	2,4 M€	216,6 M€	216,6 M€
Evolution 2019/2020	+ 533 %	-67 %	+ 14 %	+ 194 %	+ 194 %

Source : Etude LUCY menée par l'Amrae en 2021.

ETI et PME : des résultats techniques en dents de scie

Les ETI ont fait le chemin inverse : partant d'un ratio S/P très dégradé (481 % en 2019), elles sont revenues à un ratio de 85 % en 2020. La fréquence a peu augmenté (+5 %) et aucun sinistre d'ampleur n'a été déclaré en 2020 sur ce segment d'entreprise.

Quant aux PME, TPE et collectivités publiques, elles ont enregistré l'an passé 3 fois plus de sinistres qu'en 2019. Mais pour des coûts d'indemnisation qui restent limités : 40 000 € en moyenne.

Montagnes russes

Le S/P moyen du marché recouvre des réalités radicalement différentes entre grandes entreprises, ETI et PME

	Grandes entreprises	Entreprises de taille intermédiaire	PME - TPE - Public	S/P moyen
Ratio S/P en 2019	44 %	481 %	91,5 %	84,3 %
Ratio S/P en 2020	190 %	85 %	27 %	167 %

Source : Etude LUCY menée par l'Amrae en 2021.

> *En 2020, quatre sinistres XXL, indemnisés entre 10 et 40 M€ chacun, ont représenté à eux seuls 78 % du volume d'indemnisations versées.*

Des sinistres XXL à fort impact

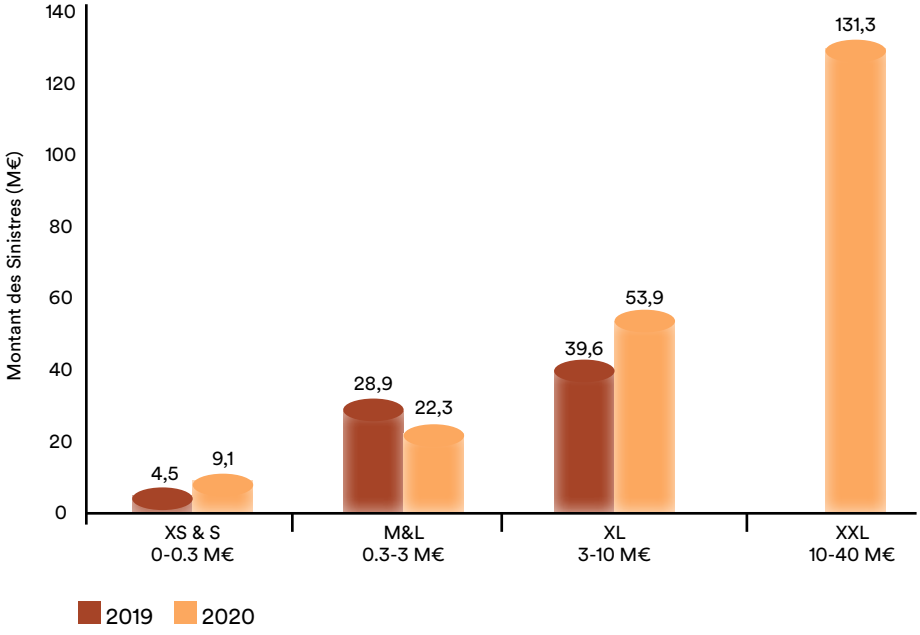
Sur l'année 2020, l'étude montre que les 80 % de sinistres de petite et moyenne intensité n'ont représenté que 4 % des indemnisations. En revanche, quatre sinistres d'intensité XXL (5,5 % des 90 sinistres enregistrés) ont représenté à eux seuls 78 % du volume global d'indemnisations versées.

Si l'on fait abstraction de ces quatre sinistres, la fréquence, l'intensité de la sinistralité et les résultats techniques de l'ensemble du marché se révèlent d'une stabilité remarquable entre ces deux exercices.

C'est l'un des principaux enseignements de l'étude LUCY : elle fait apparaître l'impact que peuvent avoir les sinistres d'intensité sur une branche d'assurance encore jeune, dont la mutualisation reste pour le moment insuffisante. Et cela confirme l'intérêt pour les entreprises de relever le niveau de leur capacité, afin d'être bien protégées en cas de sinistre d'ampleur.

Distribution des sinistres par taille d'entreprises en 2019 et en 2020 : 4 sinistres XXL changent la donne

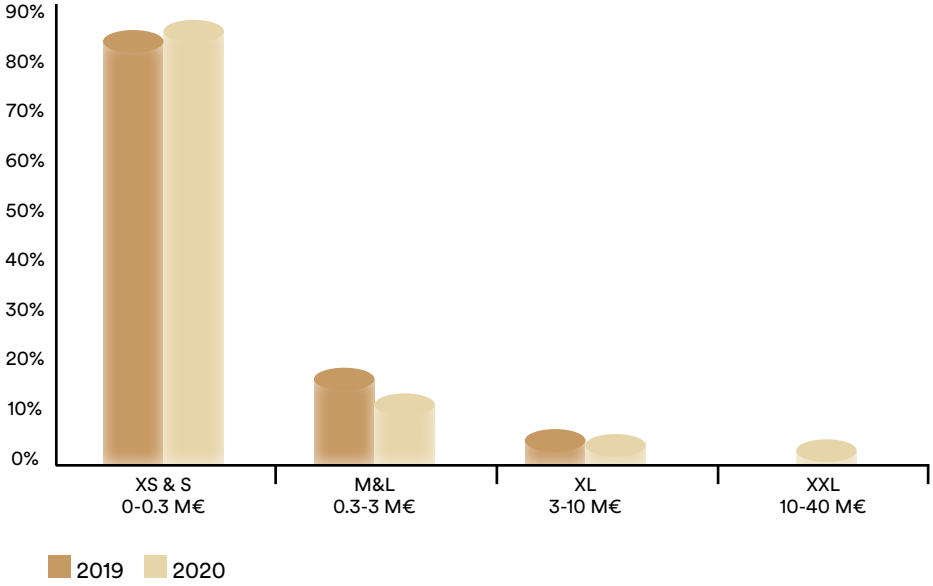
L'idée très répandue selon laquelle le nombre de sinistre cyber connait une croissance exponentielle est en partie fausse : quand on parle de sinistres de petite, moyenne ou forte intensité, la croissance du nombre de sinistres est certes réelle ; mais elle est avant tout portée par l'augmentation du nombre d'entreprises protégées. Entre 2019 et 2020, la différence se joue sur les sinistres de très forte intensité (entre 10 et 40 M€ d'indemnisation), dont le nombre est passé de 0 à 4 en un an.



Source : Etude LUCY menée par l'Amrae en 2021.

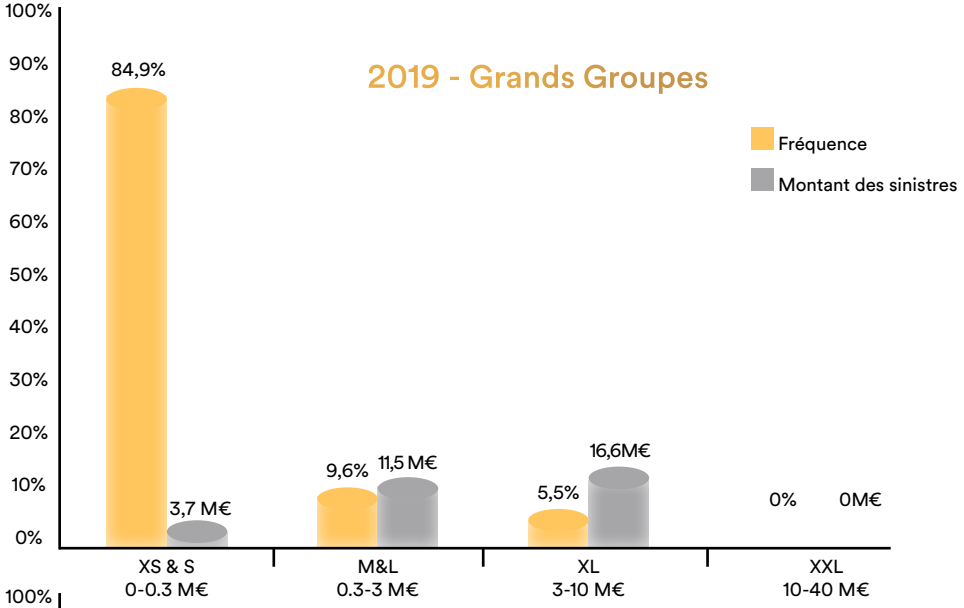
Une sinistralité stable en fréquence et en intensité... sauf pour les sinistres XXL

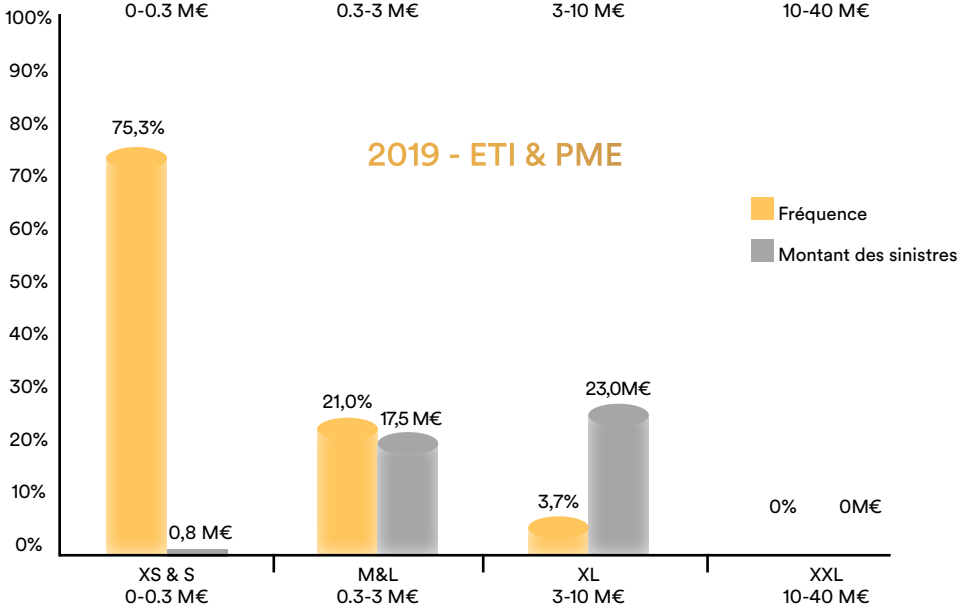
Entre 2019 et 2020, la distribution des sinistres reste stable : autour de 80 % de petits sinistres, 15 % de sinistres de moyenne intensité, 5 % de sinistres de taille L et XL. La seule différence - mais elle est de taille ! - se joue sur les sinistres XXL.



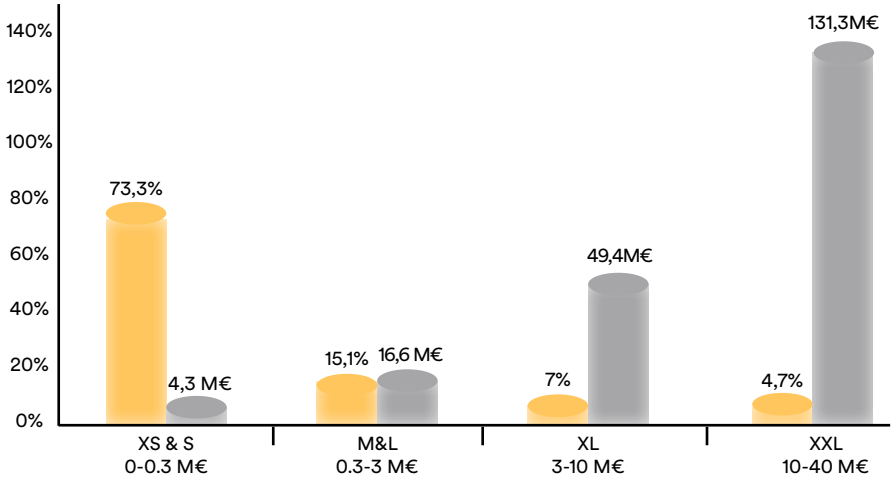
Source : Etude LUCY menée par l'Amrae en 2021.

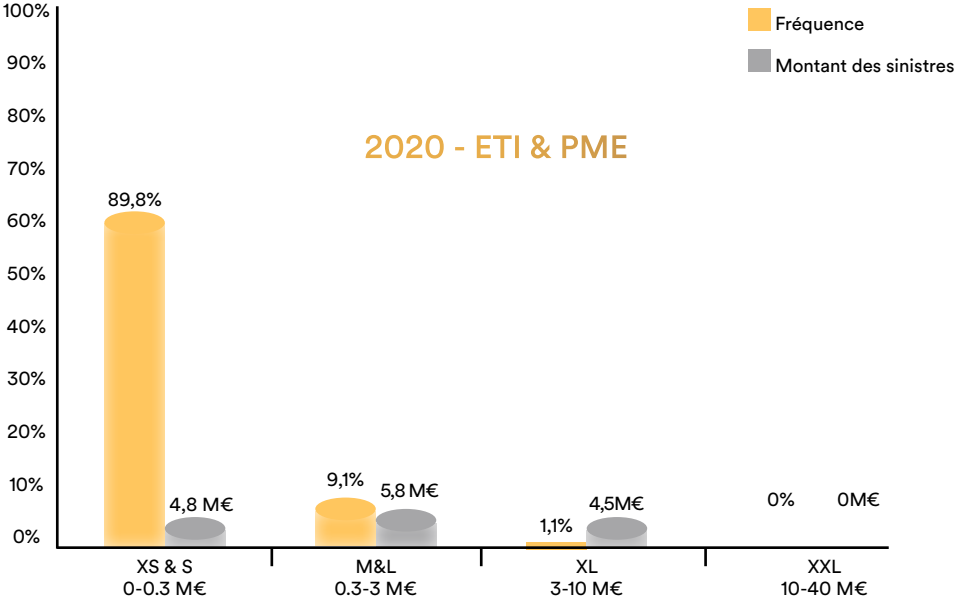
Nous allons aller plus en détail pour voir l'évolution respective des Grandes Entreprises et des ETI/PME entre 2019 et 2020.





2020 - Grands Groupes





2020 - ETI & PME

Grandes entreprises : une intensification de tous les sinistres

Si le volume des indemnisations versées aux grandes entreprises a explosé, c'est en grande partie à cause de 4 sinistres XXL indemnisés en 2020. Mais pas seulement : on observe, sur ces graphiques, un mouvement d'intensification de tous les sinistres. La fréquence des petits sinistres a chuté (de 85 % en 2019 à 73 % en 2020) alors que celle des sinistres d'intensités moyenne et forte a augmenté.

ETI : une écrasante majorité de petits sinistres

Les ETI ont nettement mieux maîtrisé leurs risques en 2020, avec une baisse très importante du volume d'indemnisations (passé de 41,3 M€ en 2019 à 15,1 M€ en 2020) due en grande partie au segment des grands sinistres, dont les coûts d'indemnisation sont passés de 23 M€ en 2019 à 4,5 M€ en 2020. Le coût des petits sinistres s'est, certes, alourdi : il est passé de 0,8 M€ en 2019 à 4,8 M€ en 2020. Mais cette hausse est loin de compenser la chute drastique des gros sinistres.

En apparence, la fréquence des sinistres indemnisés est restée stable en 2020. Avec de grandes différences entre les grandes entreprises, dont les sinistres d'amplitude ont été plus fréquents, et les ETI/PME, qui ont connu la tendance inverse. Au point que les sinistres d'amplitude et de très grande amplitude (plus de 10 M€) semblent être l'apanage des seules grandes entreprises.

Quel avenir pour la cyberassurance ?

Quel avenir pour la cyber assurance ?

Le marché de l'assurance cyber ne se consolidera que si le nombre d'assurés augmente suffisamment pour créer les conditions de la mutualisation. Mais l'équation est difficile : comment attirer davantage d'assurés quand les taux de cotisations et le niveau des franchises augmentent alors même que les limites diminuent et que les garanties s'amenuisent ?

Depuis un an, les négociations relatives au renouvellement des polices cyber sont particulièrement tendues : les assureurs proposent des augmentations de taux de cotisations que les entreprises et les collectivités publiques peinent à accepter dans un contexte économique tendu.

Les résultats de l'étude LUCY permettent de mieux comprendre ces augmentations : pour les assureurs, le ratio Sinistres/Primes est passé de 84 % entre 2019 à 167 % en 2020. Sur le segment des grandes entreprises, il a littéralement bondi, passant de 44 % en 2019 à 190 % en 2020.

S'agit-il là d'une tendance de fond ? Il faudrait deux ou trois années d'historique supplémentaire pour tirer une telle conclusion. Les résultats de l'année 2020 peuvent aussi être vus comme un accident après un cycle clément clôt par une année 2019 très positive pour les assureurs.

L'étude LUCY permet de mieux comprendre l'état du marché

Les grandes entreprises sont confrontées à un problème d'offre

Elles sont très majoritairement protégées par une assurance cyber, mais avec un niveau de couverture inférieur à leurs besoins réels. Or, les capacités disponibles sur le marché ont tendance à se contracter. De plus, les assureurs prêts à prendre le rôle d'apériteur du programme d'assurance cyber d'un grand compte (c'est-à-dire de monter en première ligne du programme) sont de plus en plus rares. Cette offre restreinte est un vrai frein au développement de l'assurance cyber, alors même que les grandes entreprises ont besoin de renforcer leur couverture.

Il faut sensibiliser les ETI au risque cyber et à sa couverture assurantielle

Au contraire des grandes entreprises, les ETI bénéficient encore aujourd'hui d'un marché concurrentiel, avec une offre importante et des prix attractifs. Si seulement 8 % d'entre elles ont souscrit une police cyber, c'est plutôt parce qu'elles méconnaissent ou sous-estiment leur exposition à ce risque. Il faut donc les sensibiliser et stimuler la demande.

Créer des offres plus adaptées aux PME

Les enseignements de l'étude LUCY sur le segment des PME sont encore limités. On peut tout de même considérer que leur taux de couverture est faible et qu'il est important de les sensibiliser aux enjeux de la sécurité numérique et de l'assurance cyber.

Il n'y a donc pas un marché de l'assurance cyber, mais deux marchés confrontés à deux problématiques radicalement différentes : un manque d'offre du côté des grandes entreprises, une faiblesse de la demande du côté des ETI, des PME et des collectivités publiques.

> *Sur le segment des grandes entreprises, les assureurs cyber ont pour la première fois en 2020 versé près de deux fois plus d'indemnisation qu'ils n'ont perçu de primes.*

En tout état de cause, les entreprises et les collectivités publiques ont, quelle que soit leur taille, intérêt à mieux se protéger contre le risque cyber en agissant sur les trois leviers : investir dans la prévention, se préparer à la gestion de crise et améliorer leur couverture assurantielle, en relevant le niveau de leur capacité pour les grandes entreprises et en augmentant le taux de couvertures des ETI/PME et des collectivités publiques.

Ce qui, dans un contexte de crise, est difficile à entendre pour les décideurs devant approuver ces évolutions budgétaires.

Les Risk Managers vont devoir trouver de solides arguments pour convaincre leur direction d'investir davantage dans la prévention et l'assurance du risque cyber, alors même que l'assurance coûtera plus cher pour des garanties équivalentes voire inférieures. Les courtiers auront intérêt à les soutenir dans cette démarche.

> *Il va falloir convaincre les entreprises et les collectivités publiques d'acheter davantage d'assurance à un prix unitaire plus élevé dans une période de grande incertitude économique...*

L'élargissement du marché est pourtant indispensable à la mise en place d'une véritable mutualisation. Mais une hausse trop importante des taux et des franchises, conjuguée à une réduction des couvertures, pourrait freiner ce mouvement.

Si le marché ne trouve pas rapidement un équilibre technique satisfaisant, les programmes d'assurance cyber vont devenir encore plus difficiles à finaliser faute d'assureurs prêts à monter en première ligne. Les renouvellements récents et les négociations en cours le montrent déjà : les assureurs préfèrent se positionner plus haut dans les programmes d'assurance, en deuxième, troisième, voire quatrième ligne pour éviter une trop forte exposition aux sinistres de fréquence, ainsi qu'à ceux de forte intensité.

L'équation à résoudre est difficile. Elle ne trouvera de résolution que dans un dialogue constructif entre assureurs, courtiers et assurés. L'étude LUCY vient nourrir ce dialogue, notamment en contribuant à définir un cadre objectif de négociation.

L'assurance cyber est un enjeu stratégique pour les entreprises et les collectivités publiques : ce qu'il faut retenir de l'étude LUCY

01. 87 % des grandes entreprises sont couvertes, ce qui montre leur conscience de ce risque. Les Entreprises de taille intermédiaire (ETI), les PME et les collectivités publiques restent moins souvent protégées.

02. Les ETI et les PME – l'essentiel du tissu économique français - ne s'assurent pas assez contre le risque cyber. Elles doivent engager le dialogue avec les assureurs et les pouvoirs publics pour trouver les meilleures solutions pour se protéger.

03. Les grandes entreprises sous-estiment encore le niveau de leur exposition au risque cyber : le montant des capacités souscrites est aujourd'hui inférieur à l'impact financier que pourrait avoir une cyberattaque.

04. 82 % du volume de primes d'assurance cyber est porté par les grandes entreprises qui ont déjà du mal à trouver les capacités dont elles ont besoin. Si l'offre de couverture cyber venait à se contracter, le marché ne trouverait plus d'équilibre.

05. Le développement de l'assurance cyber passe par une stratégie différenciée entre les grandes entreprises d'un côté, les ETI, les PME et les collectivités publiques de l'autre.

06. Le risque cyber – comme le risque pandémique - est potentiellement systémique : faute d'assurance adaptée, les entreprises et les collectivités publiques confrontées à une cyberattaque de grande ampleur verront leur avenir menacé.

07. Une offre véritablement substantielle du marché de l'assurance cyber protégera mieux les entreprises et les collectivités publiques en créant les conditions de la mutualisation indispensable à l'équilibre technique de ces garanties.

08. Le risque cyber entraîne de nombreux sinistres de faible intensité. Ceux-ci ne seront pas assurables dans la durée si les entreprises et les collectivités publiques ne mettent pas en place une véritable stratégie de sécurité numérique permettant de réduire la fréquence.

09. Une bonne préparation à la gestion de crise permet de réduire considérablement l'impact opérationnel et financier d'une cyberattaque. De ce point de vue, les intérêts des assurés et des assureurs sont parfaitement alignés : une crise plus courte permet… un retour à la normale plus rapide et un moins grand sinistre.

10. Une stratégie de maîtrise du risque cyber droit reposer sur trois piliers fondamentaux : la prévention, la gestion de crise et l'assurance.

L'institut des actuaires est particulièrement heureux de collaborer à LUCY. Pour lutter efficacement, au niveau national ou européen, contre le fléau du risque cyber, il est indispensable de disposer de données fiables sur les incidents et attaques.

Jusqu'ici, aucune base de données publique n'existait en France. L'étude LUCY constitue la première source d'information publique pour quantifier le coût économique du risque cyber auquel les entreprises sont exposées. Analyser les impacts économiques selon plusieurs critères est essentiel pour évaluer comment les risques peuvent être supportés et mutualisés. Il s'agit d'un premier pas important vers une meilleure connaissance du risque cyber, permettant une prise en charge différenciée des victimes et des cibles selon les différents niveaux d'exposition au risque.

Philippe Talleux,
Président de l'institut des actuaires

La FFA salue le travail réalisé dans le cadre de cette étude. Elle apporte une vision complémentaire à celle des assureurs sur l'évolution de ce marché. Le partage de l'information entre intermédiaires, clients et assureurs permet de bâtir les offres assurantielles les mieux adaptées aux besoins des clients.

Christophe Delcamp, FFA.
Directeur adjoint
Direction des assurances de dommages et responsabilité
Federation Française de l'Assurance

L'ANSSI a une excellente connaissance des attaques les plus sophistiquées qui visent des cibles stratégiques. Mais l'impact financier des attaques informatiques sur les entités victimes reste encore peu connu : avoir une meilleure vision des coûts contribuera à la prise conscience des organisations et aidera au développement de nouvelles solutions.

Fabien Caparros, ANSSI.
Chef d'état-major Sous-direction Stratégie
Agence Nationale de la Sécurité des Systèmes d'Information

AMRAE

www.amrae.fr

© AMRAE – MAI 2021