addactis
THE RISKTECH FOR INSURANCE

LA SOCIETE FACE AUX RISQUES CYBER

ADDACTIS France

Thomas Bastard

Emmanuelle Huguet

05 Mai 2020

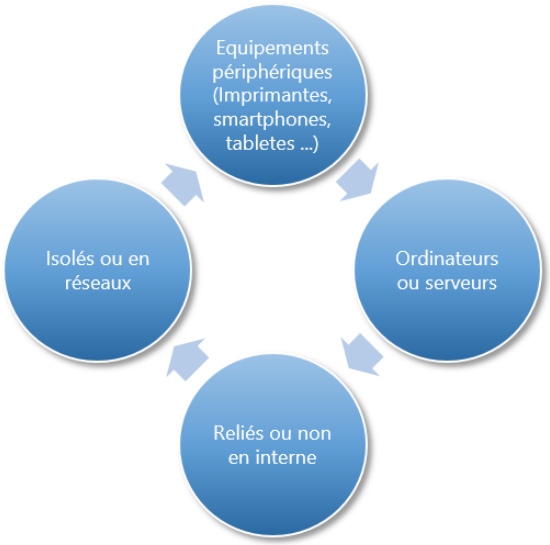
TABLE DES MATIERES

1 POUR COMMENCER

1.1 Définitions

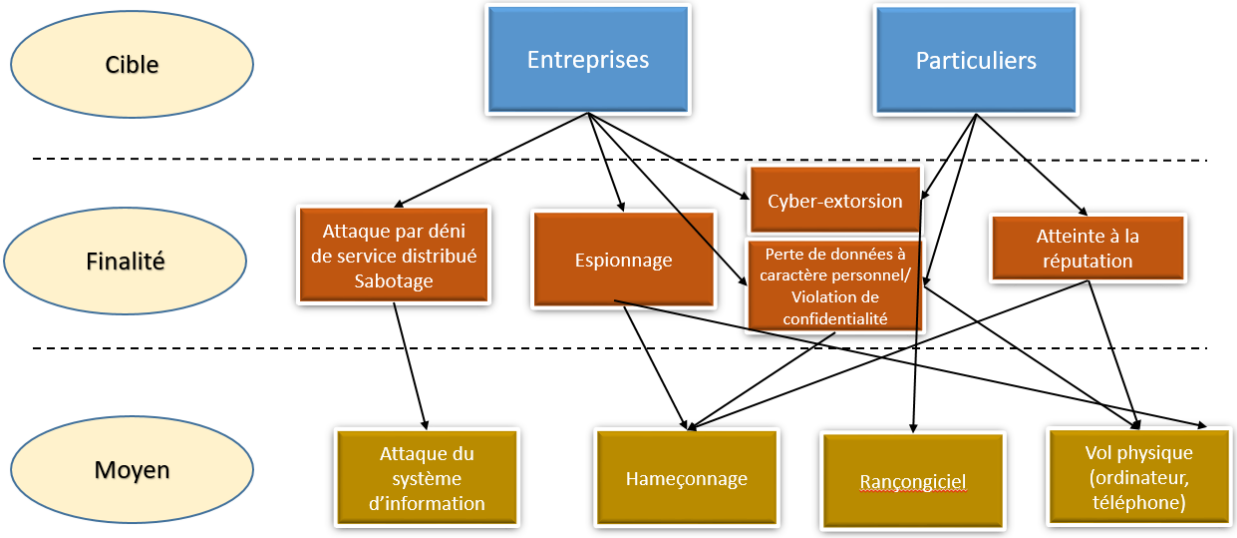
Une cyber-attaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant.

Elle cible différents dispositifs informatiques :



1.2 Les types d'attaques

Il existe plusieurs types de risques cyber aux conséquences diverses, affectant directement ou indirectement les particuliers et les entreprises. Les principaux risques et concepts sont introduits et reportés sur la figure suivante :



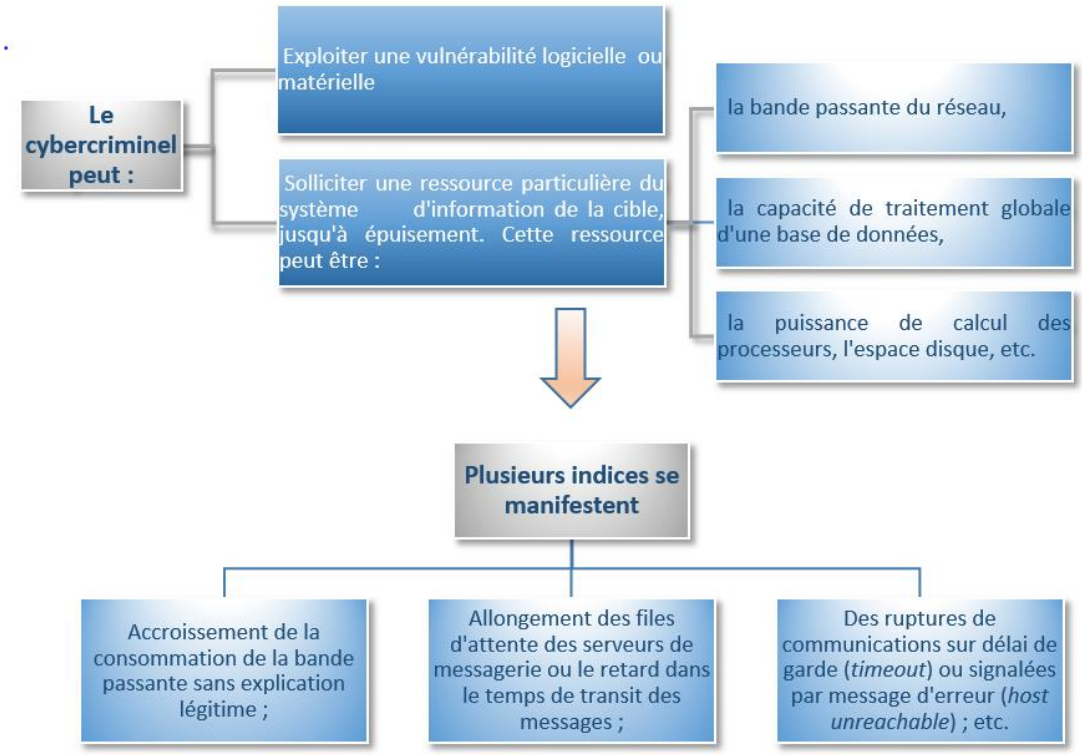
a. Attaque par déni de service distribué

Qu'est-ce que c'est ?

L'attaque de type déni de service distribué (en anglais, *Distributed Denial of Service, DDoS*) correspond à la **mise hors service** temporaire ou définitive d'un **élément opérationnel d'une entreprise**. Cela concerne le plus souvent des attaques dématérialisées (attaque d'un site web) mais cela peut également avoir pour objectif des interruptions physiques telles que la mise hors service d'un élément de production physique d'une entreprise via la mise hors service de son système informatique.

Objectif

Nuire et / ou intimider sans motivation pécuniaire (pas de demande de rançon par exemple).

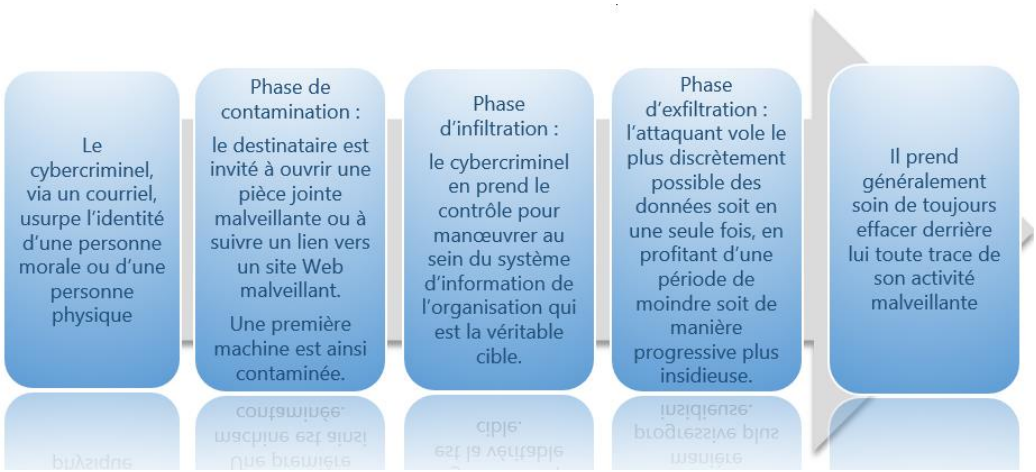


b. Espionnage

Qu'est-ce que c'est ?	Objectif
L'espionnage consiste à **extraire des informations confidentielles** d'une entreprise ou d'un acteur économique dans le but d'en tirer un **avantage économique.** Cela peut être mis en œuvre en infiltrant le système d'information (hameçonnage) ou simplement en volant du matériel informatique.	Avoir accès à **des informations économiques confidentielles** : brevets, secrets de fabrication, documents stratégiques.

❖ Hameçonnage

L'hameçonnage (*phishing*) est une technique utilisée par des Cyber attaquants pour **ouvrir une porte** d'entrée vers des systèmes d'informations en ciblant des particuliers ou des employés. L'analogie avec la pêche à la ligne vient du fait que les attaquants utilisent **un leurre** : un faux email le plus souvent. L'hameçonnage peut conduire à l'infection de machines par des *spywares* (Espionnage) ou des *ransomwares* (extorsion).



c. Cyber Extorsion

Qu'est-ce que c'est ?	Objectif
Une attaque de type cyber extorsion consiste à **bloquer** une fonctionnalité d'un site internet ou à crypter des données sur une machine, et à **demander une somme d'argent** en échange du déblocage. Des variantes consistent à menacer la victime de bloquer une fonctionnalité ou de révéler des informations compromettantes.	**Faire pression** sur la victime et l'amener à payer une **somme d'argent**.

❖ «Rançongiciel» (ransomware)

Le rançongiciel est un petit programme informatique permettant de chiffrer des données sur des machines dans le but de demander une somme d'argent à la victime. Le plus souvent, le paiement de la rançon permet le déblocage effectif des machines.

d. Perte de données à caractère personnel et atteinte à la confidentialité

Qu'est-ce que c'est ?

La perte de données individuelles avec atteinte à la confidentialité est un **vol de données à caractère personnel (DCP)**, soit massif en hackant une entreprise, soit ciblé en attaquant des individus. Ces données peuvent être de natures diverses, par exemple des **numéros de sécurité sociale**, qui permettent d'ouvrir un compte bancaire ou de faire une demande de crédit **aux USA**, ou encore des **mots de passe et identifiants** afin d'accéder à une plateforme (ex : Ebay (2014), Orange (2014), Dropbox (2016)).

Les individus sont rendus vulnérables par les entreprises auprès desquelles ils fournissent des informations personnelles.

Objectif

Revendre ou utiliser des informations individuelles. Il existe des valeurs de marché correspondant à différents types de données, facilement revendable au marché noir (***dark net***).

e. Atteinte à la réputation

Qu'est-ce que c'est ?	Objectif
Ce type d'attaque vise à porter atteinte à la **notoriété numérique** d'un individu. Cela peut se matérialiser par de la **diffamation** ou la **diffusion de contenu personnel et privé** (par exemple : vidéo à caractère sexuel).	**Nuire à un individu** dans le cadre **personnel ou professionnel.** En effet, se renseigner sur des personnes grâce à internet et désormais un réflexe bien établi.

2 UN PAYSAGE DU CYBER EN MUTATION

2.1 Le numérique transforme nos sociétés

Des attaques de grande ampleur ont révélé la fragilité de grands groupes face à l'écho médiatique : perte de confiance des clients, atteinte à la marque. Cela révèle que les **actifs intangibles** (capital intellectuel, réputation, brevets, marques, données, etc.), alors qu'ils **pèsent parfois pour plus de la moitié de la valeur de l'entreprise**, ne trouvent aujourd'hui aucune réponse assurantielle satisfaisante.

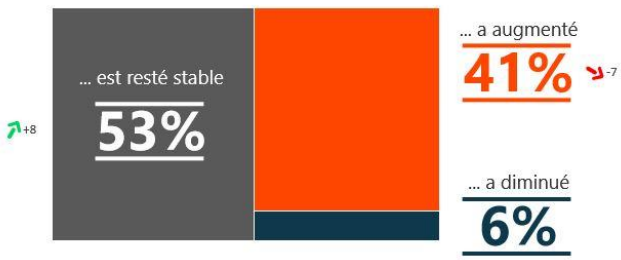
Le mariage de la nouvelle économie et de l'industrie traditionnelle (automobiles, biens domestiques) fait de la cybersécurité un enjeu auquel les développeurs, les fournisseurs de solutions et les intégrateurs ne pourront se soustraire.

En effet, l'irruption du digital dans le monde physique induit de nouveaux périls matériels et corporels et les impératifs de sécurité et de sureté (par exemple, dans les transports ou la santé) modifient la tolérance au risque. **La nouvelle économie va devoir s'adapter et son environnement juridique également.**

2.2 Le baromètre 2019

Q5BIS. Et par rapport à l'année dernière, ce nombre d'attaques constatées dans votre entreprise... ?
Base : ensemble (174 répondants)

Nombre d'attaques constatés



80 % ont subi au moins une cyberattaque en 2018

Q5. Combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?
Base : ensemble (174 répondants)

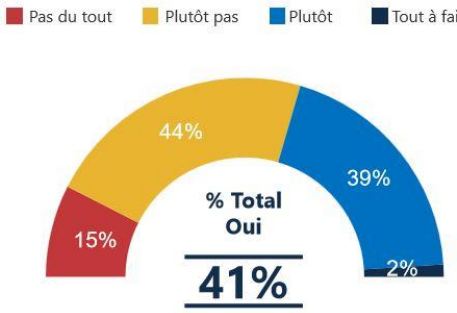
C'est le chiffre phare de l'étude. Plus impressionnants encore, **48% de ces entreprises** ont subi **au moins quatre cyberattaques** sur les 12 derniers mois.

Les attaques les plus répandues

- **Phishing** ou spear-phishing pour **73%** des entreprises touchées
- **Arnaques au président** pour **50%** des entreprises touchées
- **Infections par malware & cryptolocker ou ransomware** pour **44%** des entreprises touchées

Des solutions en matière de cybersécurité pour contrer ces attaques

« Votre entreprise est-elle préparée à gérer une cyber-attaque de grande ampleur »



Parmi les Responsables Sécurité des Systèmes d'Information (RRSI) ayant pris part à l'étude CESIN

- **56%** ont mis en place des solutions basées sur l'intelligence artificielle ou vont le faire
- **50%** des RSSI ont souscrit une cyber assurance : +10 ppts par rapport à 2017
- **10%** des RSSI ont mis en place un programme intégralement dédié à la cyber-résilience.
- **51%** des RSSI pensent que leurs entreprises sont capables de faire face aux cyber attaques : -12ppts par rapport à 2017

2.3 L'avenir de notre société face à la digitalisation

a. La Digitalisation : le changement est la seule constante

Magnétoscopes, téléphones portables avec carte prépayée, machines à écrire et lecteurs MP3 : quels sont leurs points communs ?
Ils ont disparu de nos quotidiens.
Et avec l'accélération du digitale, nombreux d'autres objets disparaitront.

Notre écosystème numérique s'est transformé suite à l'apparition de tendances technologiques, telles que le cloud, le big data, l'IA, ou encore l'IoT.

Le futur de la digitalisation apporte de nombreuses nouveautés à tous les domaines de notre vie. Les processus intelligents facilitent et optimisent notre quotidien.

En **2024, les règlements en argent liquide devraient représenter autour de 9 %** des dépenses de consommation totale des ménages en France.

Dans les dix prochaines années, la révolution digitale aura de sérieuses répercussions sur tous les domaines de notre quotidien :

Les télécommandes
A horizon 2022, on estime plus de 500 objets seront connectés par foyer

L'argent liquide
Une hausse de 74% des transactions assurées par CB a été enregistrée entre 2006 et 2015. Accélérée depuis 2015, le paiement CB sans contact et le paiement en ligne sur internet. Au global une augmentation des transactions par CB de +7% entre 2018 et 2017.

Les clés
Sécurité, personnalisation et flexibilité sont les 3 raisons du remplacement des clés par les cartes SIM, scanneurs d'empreintes digitale ou de la rétine.

Les mots de passe :
Nos appareils et comptes seront protégés par la reconnaissance faciale, vocale, digitale ou par la rétine.

La mort des tableaux en ardoise et craies en 2018
Les écoliers, collégiens, lycéens et enseignants sont déjà équipés de tablettes numériques et de ressources pédagogiques digitales.

Les distributeurs automatiques de tickets de transports
Au profit des smartphones et des QR-codes. Les e-billets rencontrent un succès grandissant.

Les lettres et les documents en papier
Adieu au fax ! L'email règne aujourd'hui en maitre.

Les chargeurs

Grâce aux nouveaux standards Qi, les téléphones portables pourront être chargés sans fil par induction.

Les taxis classiques

Des taxis autonomes sans chauffeur devraient transporter les visiteurs lors des jeux olympiques de 2021 au Japon et à Singapour.

Les interrupteurs électriques et les régulateurs de chauffage

En 2020, la domotique changera la manière dont nous vivions et 15% de tous les objets seront connectés avec une tendance à la hausse

b. Menace ou opportunité pour la CyberSécurité : la Cyber-résilience un axe majeur

Que se passerait-t-il si un attaquant accédait à distance au réseau Wi-Fi d'un avion ?

Chaque nouvelle technologie présente donc de *nouvelles opportunités pour un attaquant et de nouveaux risques cyber à couvrir.*

Comment les entreprises peuvent-elles tirer bénéfice de toute attaque subie ou déjouée pour renforcer leur cyber-résilience ?

Dans le contexte actuel, **la question n'est plus de savoir si l'on va être attaqué, mais bel et bien quand !**

Dès lors que les entreprises ont compris que **les cyber-attaques les affecteront tôt ou tard,** elles peuvent passer à l'étape suivante : la conception et l'implémentation d'un programme de Cyber-Résilience (PCR).

En permanence, il faut pouvoir :

- Identifier
- Protéger
- Détecter
- Répondre à l'incident
- Récupérer les systèmes pour garantir la continuité de l'activité

c. La 5G : Une véritable rupture technologique

En introduisant de nombreuses fonctionnalités inédites, **la 5G** n'est pas seulement une évolution de la 4G mais bien **une véritable technologie de rupture**. Son déploiement implique donc l'apparition **de nouveaux cyber-risques**, ce qui inquiète, en Europe, à la fois la communauté des télécommunications et celle de la cybersécurité.

Il s'agit de la cinquième génération de technologie réseaux mobiles, conçue pour répondre à la très grande croissance des données de nos sociétés contemporaines. Déjà commercialisée aux États-Unis, mais aussi en Corée du Sud ou encore en Suisse, elle devrait être déployée en France en 2020.

Un enjeu sécuritaire majeur pour les Etats et les grands groupes du monde entier.

Système de communication où seules les personnes qui communiquent entre elles peuvent lire les messages qu'elles échangent. Associé à son approche décentralisée (qui passe notamment par le concept de cloud computing, où des serveurs informatiques distants sont utilisés pour stocker des données émises depuis un autre endroit), la technologie pourrait donc rendre plus difficile les interceptions de communication, en l'absence de point central pour cibler une attaque.

Mais dire que la 5G sera inattaquable, C'EST FAUX.

Au-delà des débits accrus impliquant des transferts et téléchargements de données plus rapides, la 5G devrait permettre des progrès significatifs dans les domaines de l'industrie, des transports ou encore de la santé. Autant de secteurs qui devront se protéger face aux risques éventuels que posera le déploiement de cette technologie.

❖ Quels « cyber-risques » pour la 5G ?

Des risques pour les voitures autonomes

La 5G va clairement permettre et accélérer le développement *des* smart cities, avec **un impact potentiel sur la vie humaine**. Si des véhicules interconnectés n'échangent pas les bonnes informations, ou qu'on assiste à des dysfonctionnements sur les systèmes de signalisation à des carrefours, on imagine bien les problèmes que cela peut créer.

Souvent cité à titre d'exemple, l'affaire de la « Jeep » de Fiat Chryslers avait notamment fait beaucoup de bruit à l'été 2015. Deux hackers, Charlie Miller et Chris Valasek, avaient alors réussi à prendre le contrôle à distance d'un véhicule de la nouvelle série « Jeep Cherokee ».

Des risques dans l'Internet des objets

Télémédecine, pilotage de robots à distance, autonomisation des véhicules. La 5G devrait notamment servir à connecter tout un ensemble d'objets du quotidien. **C'est le fameux internet des objets** promis depuis tant d'années et que l'on commence à voir émerger aujourd'hui à travers les assistants vocaux et autres équipements intelligents. Une connectivité croissante, qui pourrait bien multiplier le nombre de failles potentielles : véhicules, accessoires du quotidien et même appareils électroménagers deviendront sujets à risque.

Différents scénarios sont d'ores et déjà imaginés par les spécialistes de la prévention : Prise en main sur les systèmes de chauffage de tous les bâtiments et déclenchement simultané pour faire tomber des cellules d'alimentation électrique, avec des effets cascade pouvant potentiellement entraîner des black-outs. Et des risques, bien sûr, pour les personnes concernées du fait des coupures d'alimentation électrique.

Des risques pour les sites industriels

Autre échelle où les risques pourraient être importants : les sites sensibles, industriels ou usiniers notamment.

La 5G impliquera en effet un nouveau déploiement plus dense d'antennes, ainsi qu'une nouvelle technologie de multiplexage (technique qui consiste à faire passer plusieurs informations à travers un seul support de transmission). **De nombreux dispositifs électroniques** utilisés dans certaines usines se retrouveront **ainsi davantage exposés, *et* donc sujets à des attaques.**

2.4 Une dynamique favorable aux attaquants

a. Un contexte économique tendu favorable aux attaques Cyber

Malheureusement la dynamique actuelle laisse envisager une croissance continue du nombre d'attaques Cyber dans les années à venir pour plusieurs raisons structurelles.

Une forte tension économique du marché du logiciel, des produits informatiques et des objets connectés.

Il reste que ces attaques sont possibles parce que des failles continuent de proliférer dans les logiciels ou les équipements IT, même si certains éditeurs ont fait de très gros progrès pour corriger leurs *bugs* et diffuser rapidement et efficacement les mises à jour de leurs produits. Mais malgré cette amélioration, ce sont encore des milliers de vulnérabilités qui sont découvertes chaque année dans les logiciels et les systèmes d'exploitation les plus courants. Et c'est sans compter les objets connectés qui sont en général très peu sécurisés.

La pression concurrentielle est l'une des principales raisons qui expliquent ce phénomène : le délai de commercialisation et la maîtrise des coûts de production sont absolument critiques. Or mettre en œuvre de la sécurité introduit des délais et des coûts (tests, audits de sécurité, application des correctifs, validation, etc.). Ainsi de nombreux produits ou services sont mis sur le marché sans que leur sécurité ne soit testée et validée.

Ensuite **la sécurité n'est pas, en général, un argument de vente très attractif,** notamment pour les produits grand public comme les objets connectés. La sécurité est vue comme une fonction non essentielle pour séduire la clientèle et n'est donc pas prioritaire dans le développement du produit.

Enfin les éditeurs de logiciels et les fabricants d'objets connectés ne subissent pas directement les conséquences des failles de sécurité de leurs produits, ils ne sont donc pas incités à améliorer le niveau de sécurité. Or à mesure de la diffusion du produit, il deviendra de plus en complexe et donc cher, de corriger ses failles.

Les attaquants jouissent d'une relative impunité :

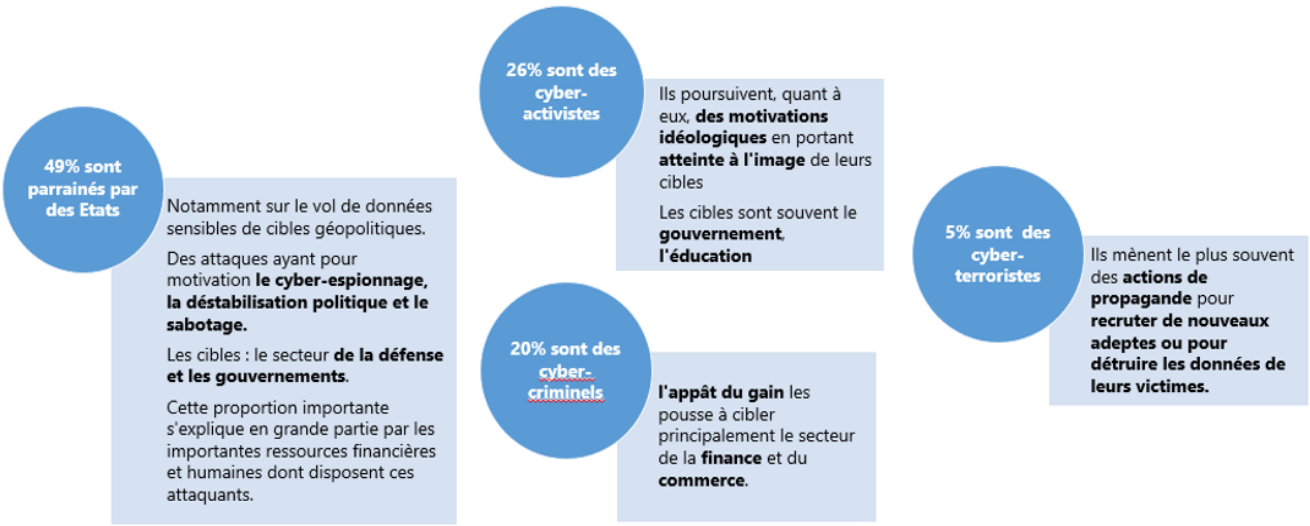
L'absence de frontières et les différences entre les réglementations nationales facilitent les actes des cybercriminels. Ils masquent leurs traces en transitant par plusieurs pays tirant parti des différences de législation rendant les enquêtes de police complexes et longues (les preuves numériques ont le temps de disparaitre).

De plus, il est techniquement **très complexe d'identifier avec certitude les criminels.** On ne dispose généralement que de preuves indirectes et insuffisantes pour identifier les auteurs avec certitude, d'autant que les codes informatiques des logiciels malveillants se recyclent ou s'échangent.

b. Une professionnalisation des cyberattaques

Les attaques informatiques sont de natures très diverses. La prolifération d'objets connectés semble stimuler l'imagination des attaquants qui réussissent à déjouer la sécurité quand elle existe de la plupart des nouveaux systèmes.

Thales et Verint ont mené une enquête de plus d'un an pour analyser et identifier les modes opératoires et les cibles des cyber-attaquants : une analyse sur 490 campagnes d'attaques dans le monde entier avec un profil détaillé de 66 groupes cyber-attaquants majeurs de haut niveau et au terme de l'analyse la définition de 4 grandes familles d'attaquants à partir de leurs motivations et objectif final.



❖ **Quelques exemples de types d'attaques organisées marquants :**

L'espionnage industriel

C'est le cas de l'affaire Boeing/ Airbus qui a vu la condamnation de Boeing à 615 millions de dollars pour avoir volé des documents stratégiques dans la négociation d'un contrat de lanceur spatial à 2 milliards de dollars.

Le sabotage

pour provoquer une désorganisation qui

C'est le cas de l'attaque menée en avril 2015 et revendiquée par DAESH contre la chaîne TV5 Monde qui a provoqué l'interruption des programmes et la diffusion de messages de propagande sur ses réseaux sociaux.

	pourra être médiatisée	Les dernières élections américaines ont par exemple été le terrain de jeu privilégié des hackers qui se sont introduits dans les boîtes mail du camp républicain.
	**Les attaques de type rançongiciel et hameçonnage** ont un but lucratif	Aujourd'hui, les mafias font des cyberattaques, peu coûteuses et qui rapportent gros. Le virus lancé le 12 mai 2017 avait pour objectif d'exiger une somme d'argent, entre 300 et 600 dollars payables en Bitcoins, par ordinateur infecté afin de récupérer l'accès à ses données.

❖ Qui est attaqué ?

La menace cyber ne concerne pas uniquement les entreprises **: aujourd'hui les** centres hospitaliers**, les** villes**, ou même les** pays **en sont les cibles directes. Les cyberattaques visent également beaucoup plus souvent des** personnes physiques **que des entreprises. Les hackers ciblent aujourd'hui en priorité** le maillon le plus faible de la chaîne sécuritaire : l'humain**.**

La diversité des secteurs attaqués cette année 2019, comme des modes opératoires démontre qu'aucune organisation n'est à l'abri d'un cyber incident. En voici quelques cas :

AIRBUS	**Janvier 2019**	Des données personnelles ont été consultées par les pirates.	Pas eu de conséquences sur les opérations commerciales.
CITY OF BALTIMORE	**Mai 2019**	Des hackers ont infiltré le réseau informatique de la ville de Baltimore et neutralisé les données de 10 000 ordinateurs municipaux pendant plus de trois semaines.	Une attaque qui a eu des conséquences importantes : impossibilité pour les habitants de payer en ligne leurs impôts et taxes, images de caméras de surveillance corrompues, incapacité des services municipaux à générer des factures. Le préjudice financier s'élève à 16 millions d'euros, s'y ajoute bien sûr le préjudice subi par les citoyens de Baltimore dont les données personnelles, notamment bancaires, ont été dérobées.
M6	**Octobre 2019**	Le groupe de médias français a été victime d'une attaque informatique, a priori via un rançongiciel	Si le groupe a pu continuer à assurer la bonne diffusion des programmes sur l'ensemble des antennes TV et radio, cette attaque rappelle la grande vulnérabilité des médias aux risques cyber.
CHU ROUEN NORMANDIE	**Novembre 2019**	Attaque informatique	Un arrêt général des équipements touchant à l'informatique, aux ascenseurs, à l'imagerie médicale, aux systèmes d'analyses… La remise en route du système a mobilisé au total une cinquantaine de personnes.

2.5 Une réglementation qui se développe face aux enjeux

a. Le règlement européen sur la protection des données (RGPD) applicable depuis le 25 mai 2018

A l'heure actuelle, en Europe, le Règlement Général sur la Protection des Données (RGPD) représente le dispositif légal de protection des données le plus avancé au monde. Il vise notamment à augmenter la protection des personnes physiques par rapport au traitement de leurs données personnelles dans tous les Etats membres.

Depuis mai 2018, tous les organismes sont soumis à une obligation de déclaration à la CNIL des violations de données personnelles dont ils auront été victimes.

La sanction est dissuasive

Les **sanctions financières** susceptibles d'être prononcées contre les entreprises sont démultipliées : jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial.

b. Le résultat des enquêtes de l'ACPR en 2019

Quelques mois avant la mise en œuvre du nouveau règlement général européen sur la protection des données personnelles (RGPD), l'ACPR a lancé une enquête sur la cyber-sécurité auprès des organismes d'assurance et de réassurance.

Peut-être est-ce un hasard du calendrier, dans tous les cas, ce qui est sûr, c'est la réalité et la permanence des risques liés aux cyberattaques qui peuvent notamment menacer directement la protection des données (*et avoirs*) de la clientèle.

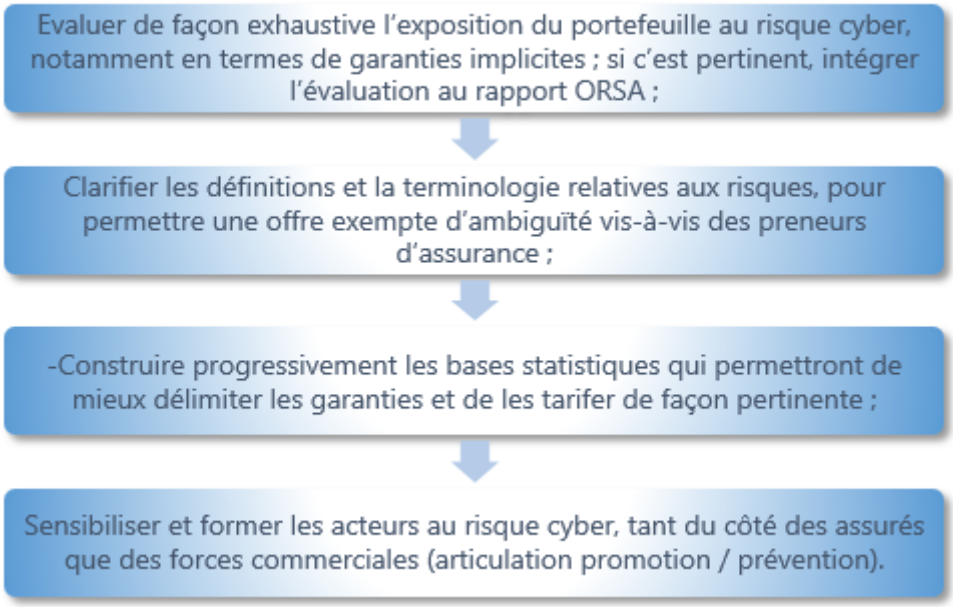
Des solutions existent pour se protéger, mais elles exigent :

- Une prise de conscience de l'ensemble des acteurs
- Une volonté de former le personnel sur ce sujet
- Et parfois, de lourds investissements en solutions informatiques.

Le 12 novembre 2019, l'ACPR a publié un communiqué sur la distribution des garanties contre les risques cyber. Clarifiant sa position sur le sujet, elle en a profité pour rappeler qu'il constituait **une de ses priorités de contrôle**.

L'ACPR a réalisé des contrôles sur la distribution de garanties contre les risques cyber sur le marché français. Si les contrats dédiés au cyber risque sont pour le moment peu développés, **les organismes ne mesurent pas encore suffisamment leur exposition**, notamment à travers les garanties implicites contenues dans les contrats en cours.

L'ACPR a identifié les axes d'améliorations suivants :



En ce sens, il existe de nouveaux périls nécessitant d'être cartographiés par les risk-managers. Ces derniers doivent alors s'assurer de la protection des **actifs dit immatériels ou intangibles**, tels que la réputation, les brevets, les marques ou encore les données de leur société qui traditionnellement ne sont pas suffisamment pris en compte dans le cadre de l'établissement de programmes d'assurance.

Sur le plan financier, les conséquences de ces nouveaux facteurs de risques tendent à remettre en cause ce que le marché de l'assurance non-vie considérait comme ses risques d'exposition les plus forts, tels que les catastrophes naturelles ou les pandémies.

Au regard des enjeux ainsi identifiés**, il peut être avancé que le risque cyber remet en cause les équilibres existants.** La véritable difficulté provient du fait que les conséquences d'un sinistre sont difficilement anticipables et peuvent prendre une dimension très importante. A titre d'exemple, l'utilisation d'un même cloud par plusieurs sociétés peut avoir pour conséquence de multiplier un sinistre affectant en chaîne plusieurs acteurs.

Ce phénomène est d'autant plus difficile à quantifier qu'il apparaît dans des circonstances qui **ne se limitent pas à des accidents aléatoires**. Certains sinistres résultent d'attaques qui peuvent provenir d'acteurs privés (isolés ou non) ou même d'organisations terroristes. En outre, la localisation et la détection de ces anomalies sont parfois rendues encore plus complexes par le fait que les auteurs du dommage peuvent mettre en place des mécanismes informatiques pour éviter toute traçabilité (utilisation de la blockchain pour les ransomwares par exemple).

2.6 Le rôle dual des États

De très nombreux États ont adopté des réglementations visant à protéger les infrastructures critiques et les données personnelles de leurs citoyens contre les attaques informatiques et **incitent ainsi les organisations publiques et privées à améliorer leur sécurité.**

Mais en parallèle, de plus en plus de pays, dont la France, annoncent publiquement développer des capacités militaires et recourir à des actions offensives dans le cyber-espace. Même si elles ont des objectifs très différents de la cybercriminalité, ces activités exploitent également les faiblesses des réseaux et des logiciels. **On peut donc s'interroger sur les priorités des gouvernements entre le besoin de sécuriser leurs citoyens et leurs entreprises, d'un côté, et celui de laisser en place des failles qui facilitent leurs actions militaires et de renseignement, d'un autre côté.**

Dans le même temps, et alors qu'aucune menace technologique n'a encore impacté à grande échelle nos sociétés, les acteurs sont face à la nécessité d'appréhender et de quantifier les événements majeurs pour évaluer leur intensité.

Ce processus pourrait conduire à la **mise en place de groupements ou d'autres structures avec garantie de l'État,** afin de répondre aux évènements technologiques d'intensité exceptionnelle, quelle qu'en soit l'origine, qui ne pourraient être portés par le seul marché commercial.
Au-delà des cyber-risques**, c'est toute l'économie du risque qui doit être repensée**, afin de prendre en compte les changements à venir induits par la technologie dans la vie des entreprises et des particuliers.

3 UN MARCHE DE L'ASSURANCE CYBER EN CONSTRUCTION

3.1 Notre appréhension face aux risques Cyber

Le cyber-risque est un risque complexe à caractère évolutif et multiforme. Cette menace émergente dont les conséquences sont aussi désastreuses que les catastrophes naturelles est un risque difficile à modéliser. Son impact n'est pas facile à quantifier, du fait qu'une attaque peut simultanément affecter une multitude de cibles.

En quelques secondes, les réseaux et serveurs informatiques de plusieurs millions d'entreprises peuvent être infectés partout dans le monde. Une offensive peut également paralyser des villes entières durant de longues périodes et se terminer par un vol massif de données personnelles.

De telles atteintes amènent certains analystes à qualifier les cyber-attaques de nouveau risque systémique.

Aujourd'hui, l'assurance et la réassurance identifient les catastrophes naturelles et les pandémies comme étant les principaux risques majeurs auxquels elles doivent faire face, **mais les risques technologiques pourraient bien changer la donne dans les années qui viennent.**

La grande perméabilité entre acteurs malveillants (États, terroristes, criminels, hacktivistes) et les moyens d'attaque rendent **l'attribution et la qualification des actes de plus en plus difficiles, voire impossibles.**

Cela questionne la segmentation traditionnelle des marchés d'assurance non-vie qui distingue classiquement accidents d'origine humaine ou naturelle, risques de guerre, terrorisme, risques politiques.

3.2 Le Marché US reste une référence

A partir de 2003, la plupart des États américains se dotent de réglementations imposant la notification aux victimes de toute compromission de données personnelles. Il est intéressant d'observer **le cycle vertueux induit par ces réglementations.**

À l'atteinte aux données personnelles se trouve associé un coût objectif : celui de la notification à des milliers voire des millions d'individus**. Cette notification démultiplie aussi le risque de réclamations et d'actions de groupe.**

Par ailleurs, **la réglementation rend publiques des attaques informatiques**, dont certaines majeures, qui étaient auparavant passées sous silence, engendrant **une prise de conscience de la part des acteurs économiques.**

La prise de conscience et le coût du risque favorisent ainsi le développement de nouveaux produits associant *:*

- La couverture des coûts propres (investigations et réparation des dommages aux données et aux systèmes informatiques)
- La gestion de crise (notification et assistance aux victimes, relations publiques, enquêtes administratives)
- Et les réclamations (frais de défense et indemnisation).

Le marché attire alors de nouveaux clients : banques et institutions financières, grande distribution, éducation, santé. Toute entreprise ayant à traiter en nombre des données personnelles s'intéresse au marché de l'assurance cyber.

Ces dernières années, le marché s'est développé selon plusieurs dimensions. En premier lieu, des attaques à fort retentissement ont rendu plus aigüe la perception du risque par les entreprises, **favorisant l'achat d'assurance.**

3.3 Le Marché de l'Assurance Cyber en phase d'expérimentation

En principe, les produits d'assurance cyber ont pour vocation de **s'adapter à ces mutations et les risques en découlant**. Ils combinent des garanties de dommages et de responsabilité pour pallier les conséquences matérielles et immatérielles des événements cyber.

Mais il faut noter que ce phénomène est insuffisamment développé. Usuellement les grands groupes se prémunissent contre les sinistres cyber alors que les PME ignorent parfois encore ce phénomène.

Il n'existe que peu de recul sur ce risque, du fait d'un faible historique de sinistralité, il n'existe pas à ce jour de bases statistiques fiables, alimentées par des données homogènes et répertoriées selon une nomenclature stable et partagée.

a. Les couvertures dites « silencieuses »

Certaines garanties sont dites affirmatives : Elles correspondent à une offre maîtrisée, l'assureur a donné une garantie en connaissance de cause et en définissant de façon positive la couverture accordée.

D'autres garanties en revanche sont implicites : elles correspondent à des garanties qui résultent de l'absence d'exclusion (ou mauvaise rédaction d'une exclusion).

On parle alors de couvertures « silencieuses ».

Au sens strict, il s'agit uniquement des dommages immatériels non consécutifs**.**

Au sens large il s'agit de tout dommage consécutif à une défaillance des Systèmes d'informations. Dès lors vont être également inclus les :

- Dommages matériels & corporels directs
- Dommages immatériels consécutifs à un dommage couvert (Typiquement PE)
- Couvert dans les polices standards DAB et RC en l'absence d'exclusion spécifique.

Ces couvertures créent des craintes chez les assureurs et réassureurs en raison du potentiel de degré d'exposition de leurs portefeuilles au risque cyber pour des polices d'assurance n'ayant pas été conçues spécifiquement pour de tels risques. Quelle attitude alors adopter ? Il existe deux méthodes employées sur le marché :

1. **La première méthode est minimaliste** en ce qu'elle consiste à **élargir les couvertures des produits** par des rachats d'exclusion ou par des extensions dédiées de garantie cyber.
2. **La seconde consiste dans la mise en place de polices spécifiques** sous forme d'un produit sur mesure / haut de gamme avec des capitaux plus importants ou garanties supplémentaires (Fraude informatique / e-reputation / RC liée au contenu internet …) ou d'un produit standard adaptés aux besoins de l'assuré.

Ce type de couverture suscite l'inquiétude des acteurs du marché. Le Lloyd's a fait récemment part de sa crainte des polices qui n'excluent pas explicitement les cyber-risques. Il a même appelé ses membres à clarifier leurs contrats d'assurance et de réassurance. Ces derniers devront dès 2020 mentionner explicitement si le risque cyber est couvert ou non et jusqu'à quel niveau.

b. L'hétérogénéité des propositions est frappante.

De petite taille, le marché de l'assurance cyber est détenu, pour l'heure, par des **assureurs extrêmement prudents.** Ces derniers font face à **un risque difficile à appréhender, évolutif et très coûteux**. De plus, l'absence d'historique sinistre peut déboucher sur une prime totalement inadaptée.

Malgré ces obstacles, la cyber-assurance se développe à un rythme soutenu. Selon les données de Munich Re, le marché est évalué à 3,5 milliards USD à fin 2018. Concentré aux Etats-Unis, la cyber-assurance va doubler son chiffre d'affaires d'ici 2020 et atteindre, toujours selon le réassureur allemand, 20 milliards USD de primes à l'horizon 2025

L'argument financier immédiat pèse toutefois lourd dans la balance. En effet, la souscription d'une **police cyber**, comme tout nouveau risque, nécessite la **création d'une ligne budgétaire nouvelle** pour les entreprises. Une **approche graduelle** est donc souvent adoptée chez les grands comptes.

Il est probable que sous la **pression, notamment des réassureurs**, les contrats évoluent assez vite, en RC comme en dommages, avec un certain nombre d'exclusions pour clarifier les textes et éviter les doublons.

Le risque cyber doit être appréhendé par secteur d'activité, avec une adaptation spécifique du fait des problématiques particulières pour chaque secteur.

c. Une cyber-réassurance encore à inventer

Jusqu'à présent, la cession du risque cyber, quand elle a lieu, se fait pour l'essentiel par extension des traités de RC professionnelle ou via quelques quotes-parts pour accompagner le développement de cédantes sur ce segment. Mais en l'absence de tailles de portefeuilles suffisantes, de modélisations crédibles et de scénarios de cumuls de risques, **la réassurance du cyber reste à construire.** À terme, les cédantes sortiront de la logique de la réassurance facultative ou de traités quote-part standards. Lorsque l'on appréhende **le cyber-risk**, nous ne sommes plus sur un produit, mais sur **un risque transverse, global** dans lequel il pourrait être envisagé des **couvertures de réassurance** dites umbrella, **couvrant l'ensemble de l'activité de l'entreprise.** Cette évolution de marché prendra toutefois plusieurs années.

4 LE CHALLENGE DES ACTUAIRES

4.1 Les critères d'assurabilité

Quantifiable	C'est à ce jour une difficulté majeure pour le cyber-risque. Peu de données sont disponibles, car le risque est relativement récent et parce que les entreprises sont réticentes à communiquer sur les attaques. Face à ces lacunes et conscientes du besoin, les institutions lancent des initiatives pour la collecte et l'anonymisation des données. Ainsi l'ANSSI a récemment mis en place le dispositif ACYMA d'assistance aux victimes qui comprend un Observatoire du risque alimenté par le recueil des données. La difficulté de ces démarches provient de leur capacité à transformer des données de bas niveau sur les incidents en informations utilisables par les assureurs (type de risques et quantification des impacts). Une autre difficulté pour la modélisation du risque provient de sa mutation dans un environnement technologique en pleine expansion. **L'expérience passée n'est pas forcément représentative du futur.**
Aléatoire	Ici l'aléa s'entend du point de vue de l'assuré, tant il est vrai que l'essentiel du risque provient de l'acte malveillant. La probabilité de succès de l'attaque repose sur le degré de maturité de la cible et la nature de l'attaquant, mais avec **une dissymétrie de moyens plutôt en faveur de l'agresseur.** Enfin certaines entreprises renommées sont la proie rêvée des hackers. Tous ces facteurs méritent d'être appréciés et modélisés. D'une façon semblable au risque politique ou au risque de guerre, dont le cyber-risque hérite en partie, il pourra s'avérer que sous certaines conditions, les facteurs de menace ou de vulnérabilité feront perdre au risque son caractère aléatoire. En segmentant par type d'activité ou en mettant en œuvre des scorings (cyber), les actuaires pourraient définir des classes de risque homogènes avec un risque aléatoire dans chaque classe.
Non systémique	L'interconnectivité grandissante des systèmes, l'utilisation de logiciels ou de matériels standards, l'externalisation croissante des services informatiques créent les facteurs de propagation des attaques et de catastrophes cyber à l'échelle planétaire, qu'il s'agisse de l'exploitation massive d'une vulnérabilité logicielle ou d'attaques ciblées sur des opérateurs qui, par leur position dominante sur le marché ou leur rôle clé dans les infrastructures techniques ou de métier, possèdent un caractère systémique. Il devient donc nécessaire dans la construction de scénarios, de **penser l'impensable.**

❖ Les capacités du marché sont-elles suffisantes ?

Il est encore rare de voir un programme d'assurance dépasser les 100 M€. Pour les dossiers extrêmes comme ceux des Gafa (Google, Amazon, Facebook et Apple), le marché fait pour l'instant un constat d'impuissance. Certains pensent que l'assurance seule ne pourra pas atteindre une capacité suffisante, même mondiale, pour supporter un sinistre chez les géants du web et que ceux-ci devront donc se tourner vers une autre solution.

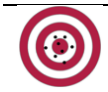
Les exclusions imposées par les traités de réassurance poussent les assureurs à se regrouper et à former des pools pour couvrir certains risques ou événements spécifiques: terrorisme, risques atomiques, risques pharmaceutiques, pollution et **à l'avenir pourquoi par le Cyber**.

Actuellement, le GAREAT structure de marché, créée fin 2001, en charge de la gestion de la réassurance des risques attentats et actes de terrorisme, a modifié son règlement intérieur à compter de 2017 et ainsi précisé les limites de sa couverture du cyberterrorisme en réécrivant son exclusion spécifique pour les conséquences des actes cyberterroristes, autres que les dommages matériels, les frais consécutifs et la perte d'exploitation consécutive légalement couverts par les assureurs, notamment sont exclus les dommages immatériels non consécutifs causés par les actes de cyber terrorisme.

4.2 Une base données exploitables

a. La base de données idéale

D'après la réglementation Solvabilité 2, la qualité des données s'apprécie au regard de trois critères :

	**Exhaustivité**	• Données permettant d'identifier les groupes de risques • Avec une granularité suffisante • Avec un historique suffisant et disponible
	**Exactitude**	• Des données adaptées à l'usage qui leur est destiné • Qui reflètent les risques auxquels est exposé l'assureur
	**Pertinence**	• Des données exemptes d'erreurs et d'omissions • Des données stockées de manière adéquate • Et qui satisfont à un niveau général de confiance

Dans le cadre du risque Cyber, les données représentent un sujet d'importance majeure: peu d'acteurs possèdent des données et le plus souvent celles-ci sont peu fournies ou de mauvaise qualité: soit les historiques sont trop faibles, soit les données sont issues de bases collaboratives et alimentées de manière hétérogène par différents contributeurs.

b. Les bases de données publiques historiques

Les bases publiques disponibles relatives à des incidents Cyber sont relatives à des incidents de type perte de données et violation de confidentialité uniquement. C'est l'un des risques Cyber majeur et le plus coûteux.

La base de données la plus connue et la plus populaire est la base PRC (Privacy Rights ClearingHouse) : Association à but non lucratif fondée en 1992 ayant pour ambition de protéger la vie privée des citoyens aux USA en fournissant les informations concernant les droits des individus ainsi que des moyens de défendre leurs droits	La base disponible gratuitement sur le site https://privacyrights.org/about De nombreuses études sont basées sur la base PRC, notamment : • [Farkas et al., 2019] Farkas, S., Lopez, O. et Thomas, M. (2019). *Cyber claim analysis through generalized pareto regression trees with applications to insurance pricing and reserving.* • [Edwards et al., 2016] Edwards, B., Hofmeyr, S. et Forrest, S. (2016). *Hype and heavy tails : A closer look at data breaches. Journal of Cybersecurity, 2:3–14.* • [Bessy-Roland et Boumezoued, 2019] Bessy-Roland, Y. et Boumezoued, A. (2019). *Modélisation stochastique individuelle de sinistres cyber.*
Une autre base moins documentée est la base VERIS community Data ou VCDB Base collaborative reportant des incidents de sécurité et basée sur un reporting standardisé. Cette collecte a débuté en 2013 et la base se concentre exclusivement sur les incidents de type perte de données.	La base VERIS est disponible sur le site http://veriscommunity.net (elle est encore gratuite) La base VERIS contient des **informations plus nombreuses** et **plus précises** que la base PRC

Le critère de qualité le plus problématique et commun à ces deux bases est **l'exhaustivité**, avec une **profondeur d'historique limitée**.

Les deux bases partagent d'autres points limitant : le fait que les **sources** ayant alimenté les bases soient **multiples** et non constantes au cours du temps posent d'importants problèmes pour mener des études sur la fréquence (***pertinence***).

Concernant les autres critères, la **base PRC** présente également un intérêt limité parce qu'elle ne contient **aucune variable de sévérité exprimée en coût** (euros ou dollars) (***exactitude***), et qu'il manque des informations importantes telles que la taille de l'entreprise.

c. La perte de données, un risque de grandes entreprises

D'après la composition de la base VERIS (données américaines) contenant des incidents ayant impliqué au moins 500 individus :

« Une grande entreprise (plus de 250 employés) a entre 100 et 1 000 fois plus de risque de subir une attaque Cyber entraînant une perte de données qu'une PME »

En effet, les PME sont moins susceptibles de détenir un nombre important de données à caractère personnel, et les attaquants ciblent les grandes entreprises.

4.3 Le rôle de l'actuaire : La modélisation

a. Les périls majeurs

Les principaux périls auxquels sont exposés les agents économiques sont :

- Les pertes de Données à Caractère Personnel (DCP)
- Les attaques par déni de service distribué
- La cyber-extorsion, via des rançongiciels

Les assureurs, via leur exposition, sont exposés à des scénarios systémiques pour chaque péril. Des approches de modélisation sont présentées ci-dessous.

	**Scénario systémique de perte de données à caractère personnel**	Un scénario systémique de type perte de données pourrait être lié à la défaillance d'un fournisseur de solution de stockage de données de type Cloud. Une approche permettant d'évaluer la **proportion d'entreprises touchées** et une évaluation du **coût par entreprise** est adaptée.
	**Scénario systémique de *Distributed Denial of Service (DDoS)***	Un scénario systémique de type perte de données pourrait être lié à la défaillance d'une plateforme de distribution de masse, que ce soit physique ou numérique. Une approche basée sur des **durées d'interruption d'activité** est adaptée.
	**Scénario systémique de rançongiciel**	Un rançongiciel performant pourrait aboutir à une proportion significative des entreprises mondiales impactée. Une approche de type **modèle épidémiologique** est adapté.

Pour les approches systémiques, il faut mélanger des jugements d'experts avec des paramètres calibrés sur des données, lorsqu'elles sont disponibles. En effet, avec seulement quelques années d'historique de sinistres, et un risque par nature très évolutif il ne serait pas adapté de calibrer un modèle sans jugements d'experts lorsque l'objectif est d'estimer un quantile de perte élevé.

Dans la suite du papier, le péril qui touche plus particulièrement les particuliers est modélisé : la perte de DCP.

b. L'exposition du particulier : la perte de données à caractère personnel (DCP)

Les variables influençant le plus la sévérité d'un sinistre et utilisées dans le modèle de tarification du risque de perte de données à caractère personnel sont :

- La zone géographique et l'environnement réglementaire,
- Le secteur d'activité de l'entreprise,
- La taille de l'entreprise,
- Le nombre d'individus dont les données à caractère personnel sont détenues par l'entreprise,
- Le niveau de maturité en cyber-sécurité de l'entreprise.

La modélisation ADDACTIS repose sur deux modèles utilisés en série :

- L'estimation du nombre de données perdues
- La modélisation du coût associé au nombre de données perdues.

❖ Modélisation du nombre de DCP perdues

Des travaux menés sur les deux bases publiques à disposition (la base PRC et la base VERIS) ont permis de proposer une modélisation du nombre de Données à Caractère Personnel (DCP) perdues lors de la survenance d'une attaque.

Intervalle de validité du modèle.

La **modélisation** s'est concentrée sur **l'intervalle** de pertes de données suivant : **[500 ; 10 millions] :**

- La borne inférieure (500) est nécessaire car les deux bases sont issues de sinistres publiés aux Etats-Unis, où la réglementation impose à toutes les entreprises la publication de leurs pertes de DCP, à partir de 500 enregistrements seulement.
- La borne supérieure (10 millions) est liée au fait que les très grosses pertes de DCP (au-delà de 1 million ou 10 millions selon les études) ont un comportement de coût différent.

Ce comportement est illustré sur la figure suivante (échelle en logarithme base 10). Sur cette figure, la grappe de points entourée en rouge se situe au-delà de la borne supérieure de **l'intervalle de confiance à 95%.** Pour éviter tout *cherry picking*, le seuil de 10 millions est retenu (en vert).

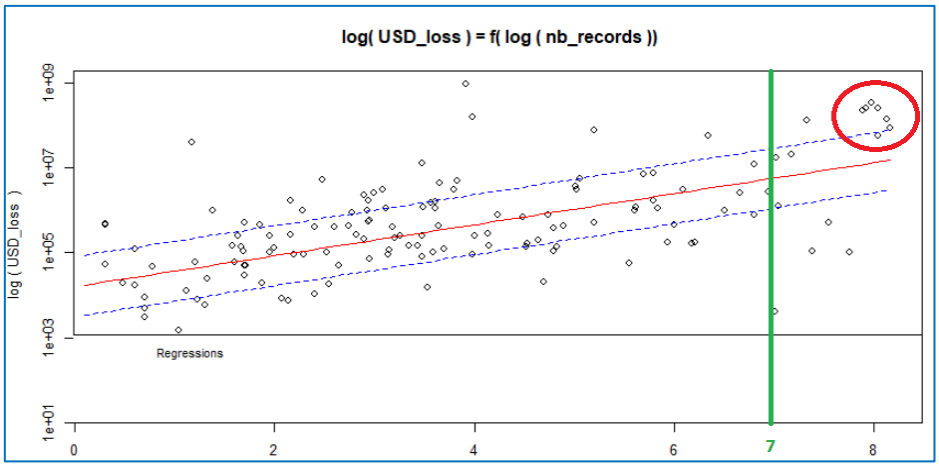


Figure 1 - Justification de l'intervalle de validité du modèle

La variable à modéliser est très dispersée. Tant dans les données VERIS et PRC, le rapport entre la moyenne et la médiane des données disponibles est de l'ordre de 1000. C'est donc le logarithme de la variable qui sera modélisé.

Prise en compte de la taille de l'entreprise sur le nombre de DCP perdues.

Tout d'abord, seule la base VERIS contient de l'information concernant la taille de l'entreprise. Une fois retraitée, la plupart des entreprises peuvent être classifiées soit Petites soit Grandes, en fonction du **nombre d'employés**, autour du **seuil de 1 000 employés**.

La première approche de modélisation retenue est l'ajustement d'une distribution au set de données. Etant donné la limitation de l'intervalle à [500 ; 10 millions], des lois tronquées ont été testées.

Huit lois ont été ajustées sur les données, pour chaque classe (entreprises Petites, entreprises Grandes) :

- Gamma et Gamma tronquée
- Log-Normale et Log-Normale tronquée
- Weibull et Weibull tronquée
- Normale et Normale tronquée

L'étude des lois Gamma et Log-Normale a permis de conclure qu'elles ont des queues trop épaisses et ne sont pas pertinentes.

Les lois tronquées apparaissent bien plus adaptées à la modélisation d'un nombre de DCP perdues sur l'intervalle choisi et à partir des données disponibles**, la taille de l'entreprise n'est pas statistiquement différenciante ici**, c'est-à-dire que l'incertitude lors de l'estimation des paramètres des lois est telle qu'il n'est pas possible de conclure que les Petites entreprises ont un comportement différent des Grandes entreprises lorsqu'elles subissent un évènement de type perte de DCP.

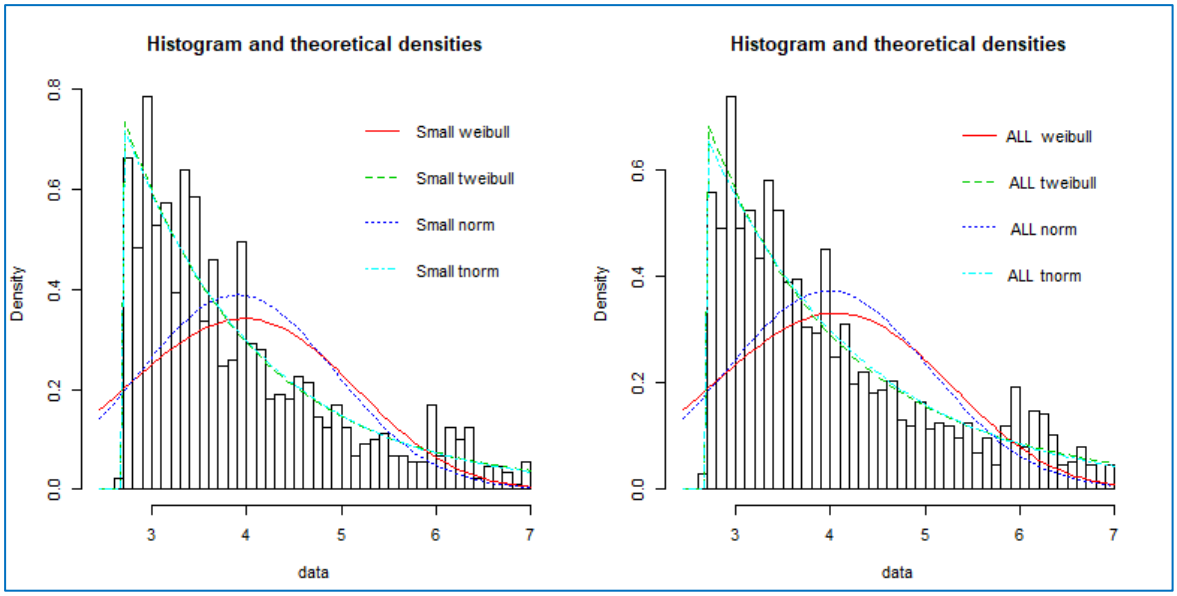


Figure 2 - Comparaison de l'ajustement des loi de Weibull et Normale, tronquées et non tronquées sur les données VERIS pour les Petites Entreprises à gauche et toutes les Entreprises à droite

La représentation graphique ci-dessus permet de constater que les lois tronquées (*tweibull* et *tnorm*) sont bien meilleures que leurs homonymes non tronqués.

Pour choisir entre *tnorm* et *tweibull*, une analyse des paramètres de la loi Normale tronquée montre que les paramètres estimés ne sont pas interprétables dans le cadre d'une modélisation sur l'intervalle [2,7 ; 7] correspondant au logarithme en base 10 de l'intervalle [500 ; 10 millions] : une moyenne négative (-44,6) et un écart-type de 8,9.

```
Fitting of the distribution ' tnorm ' by maximum likelihood
Parameters:
       estimate Std. Error
mean -44.564614   1.614005
sd     8.859047   0.205280
Fixed parameters:
      value
low 2.69897
upp 7.00000
```

La loi de Weibull tronquée apparait donc comme la meilleure pour la modélisation du nombre d'enregistrements perdus.

De plus, lorsque l'on considère uniquement les entreprises Petites (à gauche) ou toutes les entreprises (Petites et Grandes, à droite), les distributions semblent similaires.

Ces deux points (les lois tronquées sont meilleurs, et les distributions Petites versus Petites et Grandes) ont été vérifiés statistiquement.

Attention, nous ne concluons pas ici que la taille de l'entreprise n'influe pas sur le risque.

Tout d'abord, le seuil disponible dans la base VERIS (1 000 employés) n'est pas en ligne avec la définition d'une grande ou petite entreprise de l'Union Européenne : une Petite entreprise est composée au maximum de 49 employés, une Moyenne entreprise au maximum de 249 employés. A partir de 250 employés, l'entreprise est Grande.

Dans les classes disponibles dans la base VERIS, la classe Petite contient donc des grandes entreprises au sens de l'Union Européenne.
De plus, en considérant que d'après les statistiques de l'OCDE

(https://stats.oecd.org/Index.aspx?QueryId=81354&lang=fr), il y a 4.215.610 PME (< 250 employés) aux Etats-Unis et 26.144 grandes entreprises (250 employés ou plus) en 2015. En France en 2017, il y a 2.741.040 PME et 4 034 grandes entreprises. Il y a donc 163 fois plus de PME que de grandes entreprises aux Etats-Unis et 680 fois plus en France !

Or, la base VERIS reporte plus d'incidents concernant des grandes entreprises (> 1 000 employés) que d'incidents concernant des petites entreprises (< 100 employés) : 1 192 Petites entreprises (> 1 000 employés) et 1 410 Grandes entreprises (1 000 employés ou plus).

Cela signifie, qu'en termes d'ordre de grandeur, une grande entreprise a entre 100 et 1 000 fois plus de risque de subir une attaque entraînant une perte d'au moins 500 DCP.

Un nombre important de PME ne sont pas à risque car elles ne collectent pas de DCP, ou trop peu de DCP par rapport au seuil de 500. Le résultat ci-dessus est donc intuitif.

De manière générale, comme une entreprise ne peut pas perdre plus de DCP qu'elle n'en héberge, l'utilisation de ce modèle **pour une entreprise spécifique** est limitée à l'intervalle : **[500 ; min (nombre de DCP maximal à risque ; 10 millions)**].
Le modèle utilisé par la suite est basé sur une loi de Weibull tronquée sur l'intervalle [500 enregistrements ; 10 millions enregistrements] afin de modéliser le logarithme (en base 10) du nombre d'enregistrements.

Pour les entreprises qui ne possèdent pas 10 millions d'enregistrements, l'intervalle est ajusté de telle sorte à ne proposer que des **tirages adaptés au profil de l'entreprise** : **[500 ; min (nombre de DCP maximal à risque ; 10 millions)**].

❖ Modélisation du coût (en euros / dollars)

- La modélisation du coût repose sur la calibration d'un **modèle développé dès 2014 par Jacobs** [*Jacobs, 2014] Jacobs, J. (2014). Analyzing ponemon cost of a data breach*, de la forme :

$$\log(coût) = \mathrm{a} + \mathrm{b} * \log(nb\ enreg.) + \varepsilon \qquad (Jacobs)$$

$$\text{Avec } \varepsilon \sim Normale\ (0\ ;\ \sigma^2)$$

  Ce modèle repose sur trois paramètres : $(\boldsymbol{a}; \boldsymbol{b}; \boldsymbol{\sigma})$ **.**

- Un autre type modèle a été calibré sur les données de la base VERIS, **le modèle de Farkas** (2019) :

$$\log(coût) = \mathrm{a} + \mathrm{b} * \log(\log(nb\ enreg.)) + \varepsilon \qquad (Farkas)$$

  Sur le graphe ci-dessous, VERIS_1 et VERIS_2 correspondent respectivement au modèle Jacobs et Farkas calibré avec les données VERIS.Jay Jacobs a recalibré son modèle sur une base plus fournie en 2015 : JJ_old correspond à la calibration de 2014, JJ_update à la calibration de 2015.

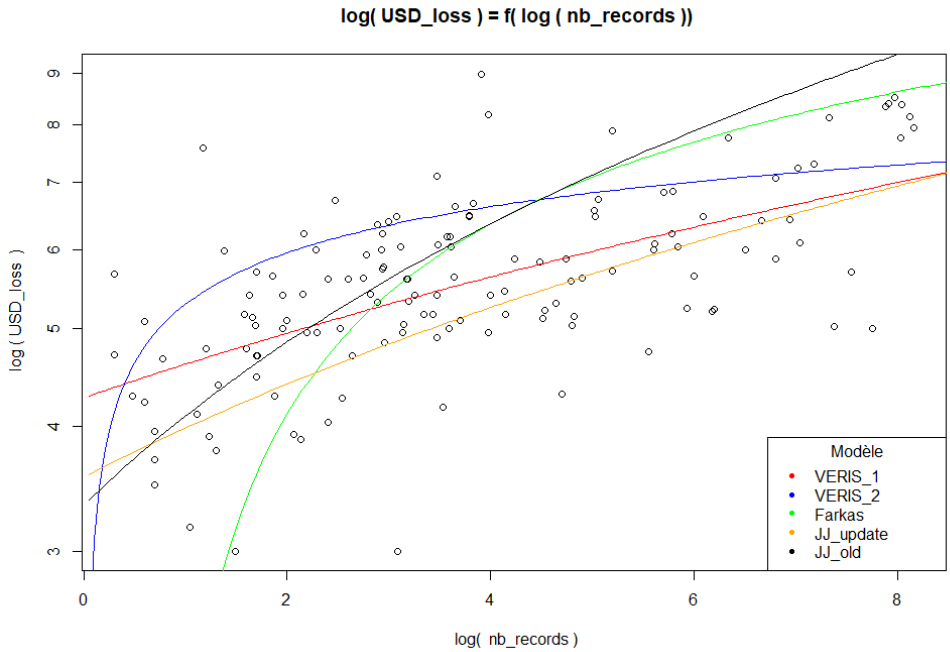


Figure 3 - Les différents modèles existant comparés aux données VERIS

Pourquoi recalibrer un modèle existant ?

Les données VERIS sont plus récentes et recueillent un nombre plus important de données.

Choix du modèle : La structure de modèle de Jacobs est plus pertinente que la structure du modèle de Farkas.

log - log	param1	param2	résidus	σ	Plage de validité
JJ 2015	8,194	0,424	normal	1,574	1 à 100m
JJ 2014	7,680	0,760	normal	0,523	1 à 100k
VERIS fit (1)	9,831	0,342	normal	2,287	1 à 10m

Figure 4 - Calibration du modèle de Jay Jacobs sur les données VERIS

Les trois paramètres sont nécessaires pour pouvoir lier nombre d'enregistrements perdus et coût financier moyen.

Pour un **nombre de DCP fixé noté n, la variable coût suit une loi log-normale** de paramètres $(\mu; \sigma^2)$, avec $\mu(n) = a + b * \log(n)$

et l'espérance du coût vaut :

$$\mathbb{E}[coût] = e^{\mu(n)+\frac{\sigma^2}{2}}$$

L'espérance $e^{\mu(n)+\frac{\sigma^2}{2}}$ est plusieurs fois supérieure à la médiane $e^{\mu(n)}$: un rapport 5 pour le modèle de Jacobs (2015) et un rapport 10 pour le modèle calibré avec les données VERIS.

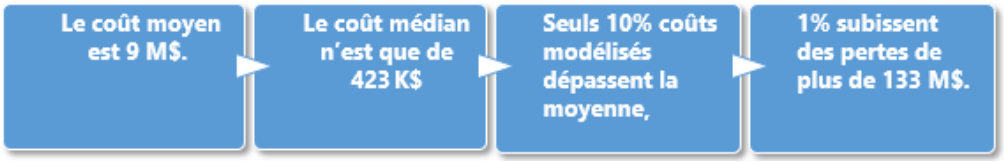
❖ Prise en compte des autres spécificités d'une entreprise

Les autres spécificités (zone géographique et l'environnement réglementaire, secteur d'activité et niveau de maturité en cyber-sécurité) sont prises en compte grâce à un ajustement proportionnel du coût issu du modèle de coût.

Ces ajustements sont basés sur une étude d'IBM et de Ponemon (2019). Cette étude précise par exemple qu'une DCP perdue coûte en moyenne 48 % de plus aux Etats-Unis qu'en France (242 $ contre 163 $), qu'une perte de DCP dans le domaine de la santé coûte en moyenne 71 % qu'une perte de DCP d'une entreprise du domaine des transports.

❖ La sévérité du risque de perte de données, coûteuse et fortement dispersée

D'après le modèle de sévérité, sur un incident de type perte de données d'au moins 500 DCP aux Etats-Unis pour une entreprise du secteur médical, de cyber-maturité moyenne et exposée à des pertes maximales de 10 millions d'enregistrements :



❖ Modélisation de la fréquence

La base VERIS comme la base PRC ne sont pas adaptées à la calibration d'un modèle de fréquence.

En effet, ces deux bases souffrent de biais importants, notamment liés à la source d'acquisition des données. Ces bases agrègent des informations issues de données fédérales, de données de chacun des 50 Etats des Etats-Unis, de médias, d'ONG et d'autres sources encore. La contribution de chacune de ces sources est trop fluctuante au cours du temps pour estimer une fréquence sur ces données.

Les résultats d'une étude quantitative du CESIN (Club des Experts de la Sécurité de L'information et du Numérique) ont été utilisés pour estimer la fréquence. Cette étude de 2019 est issue d'un sondage réalisé par OpinionWay auprès de 174 entreprises représentatives du risque des grandes entreprises.

A partir de cette étude, une hypothèse de fréquence a été calibrée : le processus de fréquence de survenance d'un sinistre pour une grande entreprise suit une loi de Poisson de fréquence annuelle 0,42.

c. La réassurance

Actuellement, le marché de la **réassurance** est majoritairement composé de **couvertures proportionnelles**, ce qui est caractéristique de risques peu connus du marché.

Dès lors qu'il existe un modèle permettant une modélisation *From Ground Up* d'un risque, il devient possible de proposer une modélisation d'un **risque Cyber**, avec une

approche simulatoire coût – fréquence, appliquée à la **tarification d'une couverture en excédent de sinistre.**

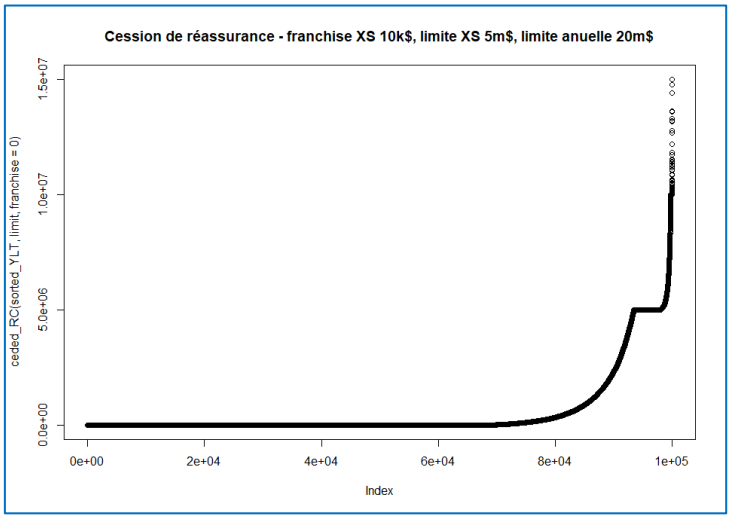


Figure 5 - Cession de réassurance, étude de cas d'une grande entreprise aux Etats-Unis du secteur médical

❖ Prime pure et chargement pour risque

- La prime pure (la moyenne des coûts annuels simulés) vaut 590k $.
- L'écart-type des coûts simulés vaut 1,5m $.
- Sous l'hypothèse d'un chargement égal à 50% de l'écart-type de la distribution, on aboutit à un prix (hors chargements pour frais) de 590k$ + 50% * 1,5 m$ = 1,34m$.

❖ Analyse

Ce prix est plus élevé que les prix de marché. Cela s'explique tout d'abord par les hypothèses initiales :

- L'entreprise considérée évolue aux Etats-Unis dans le secteur médical, qui sont des entreprises pour lesquelles les pertes de DCP coûtent particulièrement cher.
- Le choix du traité : les limites XS et annuelles sont élevées, ce qui concourent à une prime pure élevée et à un écart-type élevé. Dans cet exemple, **le chargement pour risque est supérieur à la prime pure**, caractéristique d'un risque très volatil et incertain. Ce qui explique la forte proportion de capacité de réassurance proportionnelle sur le marché français.
- Enfin, le prix du marché ne reflète pas forcément correctement le risque et peut être sous-évalué.

d. Les mega-pertes de données

Les méga-pertes de données sont les attaques impactant les données d'au moins 1 million de DCP.

Le modèle présenté ci-dessus permet de modéliser des méga-pertes de données jusqu'à 10 millions. La première difficulté de l'estimation du coût de ces sinistres est le faible nombre de sinistres historiques.

Des études des méga-pertes existent, par exemple l'institut **Ponemon, en collaboration avec IBM,** estime que le coût moyen par individu varie **de 42 $** (1 million d'individus) **à 8 $** à partir de 50 millions.

Les chiffres de Ponemon ont été **calibrés sur seulement 14 entreprises** ayant rencontré ce type de pertes.

Le modèle de coût présenté ci-dessus estime également que le coût moyen par donnée compromise est décroissant, **de 29 $** pour les plus petites méga-pertes (1 million de DCP) à 6 $ pour les méga-pertes de 10 millions de DCP, pour une entreprise située aux Etats-Unis.

$$Coût\ moyen\ d'une\ DCP(n) = \frac{e^{\mu(n)+\frac{\sigma^2}{2}}}{n}$$

Avec *n* le nombre de DCP.

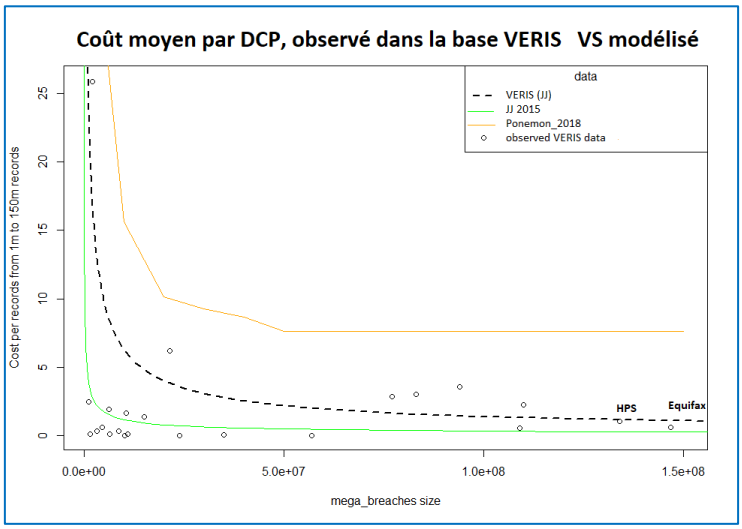


Figure 6 - Coût par DCP, données VERIS, modèle JJ (2015) et modèle de coût de l'étude

Attention, sur la figure ci-dessus les modèles de Jacobs (2015) et calibrés sur la base VERIS ont été étendus au-delà de leur plage de validité à titre informatif (respectivement jusqu'à 100 millions et 10 millions de DCP).

Ce graphe permet d'observer que les chiffres Ponemon sont nettement plus élevés que les montants présents dans la base VERIS.

Les deux plus gros sinistres du graphe, Equifax (143 millions d'individus, 2017) et Heartland Payment Systems (134 millions, 2009) n'ont coûté respectivement que 87,5m $ et 140m $ soit 0,61 $ et 1,04 $ par individu.

Dans le cadre d'une modélisation actuarielle, l'étude des méga-pertes de DCP n'est pas essentielle, ces incidents rares et les polices d'assurance comme les traités de réassurance proposant des limites significativement plus faibles que les montants en jeu.

4.4 La réponse à l'enjeu réglementaire

a. Les recommandations de l'ACPR

L'ACPR invite les acteurs à évaluer de façon exhaustive l'exposition au portefeuille cyber, notamment en termes de garanties implicites. Cette exposition peut être réalisée notamment au travers de la surveillance produit prévue par la Directive sur la distribution d'assurance (DDA). **L'ACPR propose d'inclure le risque Cyber dans le rapport ORSA.**

En outre, il est préconisé de clarifier les définitions et la terminologie relatives aux risques pour permettre une offre exempte d'ambiguïté vis-à-vis des preneurs d'assurance. On notera que le code des assurances requiert notamment que les exclusions soient formelles et limitées pour être opposables ou que l'objet des garanties soit clairement défini.

Sur le plan actuariel, il est recommandé une construction progressive des bases statistiques. Ce qui permettra de mieux délimiter les garanties et de les tarifer de façon pertinente.

Enfin, l'ACPR note que le marché a mis en place des organisations ad hoc pour la conception et la rédaction des garanties d'assurance combinées avec des actions de sensibilisation et de prévention lors de la souscription. Dans ce cadre, le régulateur enjoint à une sensibilisation et une formation des acteurs au risque cyber tant du côté des assurés que de celui des forces commerciales.

b. Le besoin global de Solvabilité

Dans le cadre de l'exercice du Besoin Global de Solvabilité (BGS) de l'ORSA, l'organisme d'assurance doit évaluer son *profil de risque*, c'est-à-dire proposer une évaluation et un suivi de tous les risques susceptibles d'impacter son niveau de fonds propres, ainsi que lister les moyens d'atténuation et de transfert de risque.

Le risque Cyber est à considérer comme certains autres risques qui ne sont pas pris en compte dans le Pilier 1 et qui sont généralement inclus dans le BGS tels que :

- Le risque de liquidité,
- Le risque des spreads souverains,
- Le risque de réputation et les risques stratégiques,
- Le risque d'évolution de l'environnement légal,
- Le risque d'inflation.

❖ Un exemple de scénario ORSA, selon les caractéristiques de l'entreprise : taille, exposition et niveau de Cyber-vulnérabilité :

*Suite à un incident lié à un **dysfonctionnement du site internet** d'un assureur MRH, il devient possible d'accéder à l'espace personnel en ligne de n'importe quel assuré sans rentrer le mot de passe, mais simplement en remplissant un formulaire de devis, puis en rentrant l'adresse email de ce dernier. Le site connecte alors directement l'individu ayant fait la demande de devis au compte personnel de l'assuré. Le dysfonctionnement est signalé par un particulier directement au service client de l'assureur, surpris du dysfonctionnement.*
*Près de **100 000 assurés** sont théoriquement impactés par le dysfonctionnement. Par mesure de sécurité, le site internet est **coupé pendant 24h** par les équipes IT, et un audit du site internet est engagé.*
*La perte pour l'assureur est évaluée à **600 000 € pour l'audit** du site et **1 million d'euros de perte d'exploitation** pour les 24h d'indisponibilité du site internet. **Des frais annexes (95 020 €)** sont engagés pour la mise en place d'actions correctives et le signalement de l'incident aux autorités compétentes.*

Ces coûts sont issues d'une **table de sévérité de référence adaptée au spécificité de la société**, et représente le coût du risque opérationnel de cyber-attaque de type perte de DCP.
La table de sévérité ci-dessous représente des coûts associés aux quantiles, pour différentes tailles de perte de DCP :

- ✓ A pour une perte de 100 DCP,
- ✓ B pour 1000,
- ✓ jusqu'à F pour 10 millions de DCP.

Le scénario ci-dessus correspond à une perte de 100 000 DCP et un quantile à 60 %, soit 1 695 020 euros de coût total.

	Scénarios et coûts associés selon le quantile					
Quantile	A	B	C	D	E	F
10,0%	4 786	10 508	23 072	50 660	111 234	244 236
20,0%	13 089	28 739	63 102	138 554	304 222	667 979
30,0%	27 038	59 367	130 352	286 214	628 440	1 379 865
40,0%	50 257	110 348	242 291	531 998	1 168 107	2 564 811
50,0%	89 707	196 969	432 484	949 604	2 085 043	4 578 125
60,0%	160 124	351 584	771 973	1 695 020	3 721 751	8 171 841
70,0%	297 629	653 504	1 434 897	3 150 602	6 917 770	15 189 333
75,0%	419 516	921 131	2 022 527	4 440 858	9 750 782	21 409 773
80,0%	614 822	1 349 963	2 964 111	6 508 293	14 290 246	31 377 065
85,0%	959 937	2 107 732	4 627 944	10 161 566	22 311 731	48 989 824
90,0%	1 681 520	3 692 109	8 106 757	17 799 990	39 083 402	85 815 348
95,0%	3 859 624	8 474 568	18 607 592	40 856 654	89 708 873	196 973 596
96,0%	4 916 557	10 795 274	23 703 163	52 044 987	114 275 076	250 913 557
97,0%	6 620 457	14 536 525	31 917 818	70 081 891	153 878 668	337 871 087
98,0%	9 832 696	21 589 632	47 404 312	104 085 555	228 540 446	501 805 804
99,0%	18 341 147	40 271 621	88 424 319	194 153 101	426 301 580	936 029 535
99,5%	32 450 344	71 251 157	156 446 025	343 508 226	754 240 331	1 656 084 002
99,9%	105 230 242	231 053 833	507 324 443	1 113 931 275	2 445 856 693	5 370 362 695

❖ Approche BGS

Dans le cadre du BGS, une fois les scénarios centraux et stressés calibrés il devient possible :

- D'ajouter ce risque aux **projections du *Business Plan***
- D'imputer le chiffre d'affaires de la société
- De refaire les calculs en environnement dégradé
- De mener une **réflexion** sur les **mesures d'atténuation du risque**
- De mener une **réflexion** sur les **mesures de transfert de risque**

Afin de respecter l'appétence, les tolérances et les limites au risque de la société.

5 POUR CONCLURE

5.1 Une culture du risque Cyber à construire

Les deux enjeux du risque Cyber sont le caractère évolutif du risque et le partage d'informations.

Les données propres aux organismes d'assurance ne suffisent pas, il faut utiliser des données externes. Il existe deux types de données externes, selon la manière dont elles ont été collectées : **les bases publiques et les bases issues de consortiums :**

- Les **bases publiques** utilisent les informations médias et / ou sont alimentées par différentes contributeurs, elles sont **accessibles à tous** et peuvent être gratuites ou payantes.
- Les **bases issues de consortiums**, alimentées par des abonnés dont les contributions sont anonymisées. Tous les abonnés partagent leurs informations sur un fichier central, et **seuls les abonnés** ont accès à la base.

Par analogie avec la gestion du risque opérationnel dans le domaine bancaire, il existe une base de référence publique, FIRST (par IBM) qui est une base publique, et ORX (Operational Risk eXchange Association). Bâle II a favorisé l'utilisation de la base ORX.

Chaque base est susceptible d'être biaisée, mais de manière différente :

- Les **bases publiques** contiennent généralement une surexposition de **gros évènements**, typiquement reportés **dans les médias**,
- Les **bases par consortiums** sont susceptibles de contenir des biais lorsqu'elles sont alimentées par **peu d'abonnés**, mais sont plus représentatives du risque.

5.2 ADDACTIS Cyber Community

ADDACTIS France va lancer au deuxième trimestre une *Cyber Community*, dont les objectifs sont de :

- Favoriser la diffusion de la connaissance du risque Cyber auprès du marché,
- Créer des synergies entre les différentes visions et les connaissances des différents acteurs : courtiers, assureurs, mutuelles, réassureurs, consultants
- Favoriser les échanges entre experts liés au sujet : experts en cyber-sécurités, chercheurs, actuaires, souscripteurs.

5.3 ADDACTIS France vous accompagne

addactis
THE RISKTECH FOR INSURANCE

ADDACTIS France propose d'accompagner ses clients

pour proposer des scénarios probables, centraux et pessimistes, adaptés au profil de risque de chaque organisme,

en s'appuyant sur sa connaissance du risque Cyber de type pertes de données et violation de confidentialité.

ADDACTIS France recommande

une approche où **l'organisme estime des nombres de données perdues probables adaptés à sa situation** propres (par exemple son nombre d'assurés).

Et à partir **d'une table de sévérité de référence calibrée par ADDACTIS France et d'ajustements spécifiques à l'entreprise**, il est **possible d'associer un coût** aux scénarios retenus par l'assureur.

L'estimation de ces coûts est **complétée de bonnes pratiques d'atténuation du risque et de transfert de risque.**