IRM | institut du risk management

Rapport de projet présenté devant un Jury de Soutenance

Expert ERM

Expert(e) Management des Risques Financiers et Assurantiels

Le 18/11/2021

Par : Amine Cherquaoui

Titre : Démarche ERM en réponse au risque de perte de données sensibles résultant d'une stratégie de digitalisation au sein d'une compagnie d'assurance

Confidentialité : ■ NON ☐ OUI (Durée : ☐ 1an ☐ 2 ans)

La durée de confidentialité expire aux 31 décembre N+1 (1 an) ou N+2 (2 ans)

Les stagiaires s'engagent à ce que les données de l'Entreprise présentées dans le cadre des travaux de la formation (rapport de projet & présentation) respectent les règles relatives à la protection des données à caractère personnel conformément aux dispositions de la Loi informatiques et Liberté n°78-17 du 6 janvier 1978 modifiée par la Loi du 6 août 2004 ainsi que par la loi n° 2018-493 du 20 juin 2018 (RGPD)

Membres présents du jury :

_____

_____

_____

_

_____

_____

Par ma signature j'autorise la publication sur un site de diffusion de documents actuariels du rapport de projet
(après expiration de l'éventuel délai de confidentialité)

Nom : CHERQUAOUI

Prénom : Amine

Signature du stagiaire

Remerciements

En premier lieu, je tiens à remercier sincèrement Pierre AURELLY, mon tuteur de mémoire, pour sa disponibilité, le temps qu'il a consacré à m'orienter, me challenger, me relire et les précieux conseils et expériences qu'il a su partager.

Un grand merci aussi à l'ensemble de mes amis, collègues, clients que j'ai sollicités et qui m'ont permis de réaliser ce mémoire tant par leurs partages d'informations, leurs remarques pertinentes et leurs soutiens, merci tout particulier à Mehdi T., Mounir Bellmane, Marc-Antoine Defransure, Antoine Kahn.

Je remercie également ma hiérarchie pour leur confiance et leur disponibilité, notamment Bertrand Pitavy et Alessandro Santoni.

Merci à tout ceux qui m'ont soutenu de près ou de loin à la réalisation de ce présent mémoire.

Enfin un grand merci à mon épouse et ma famille, merci pour vos encouragements et votre patience.

Sommaire

I. Introduction

La digitalisation des activités économiques et sociales a contribué à l'augmentation du cyber risque. Une Cyber-attaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant ciblant différents dispositifs informatiques : des ordinateurs, des serveurs, isolés ou en réseaux, reliés ou non à Internet. Les entreprises sont principalement exposées à quatre types de Cyber-attaques (détaillés en Annexe1) : l'exfiltration de données (en particulier les Données à Caractère Personnel), la perte de données, l'attaque par déni de service et la Cyber-extorsion.

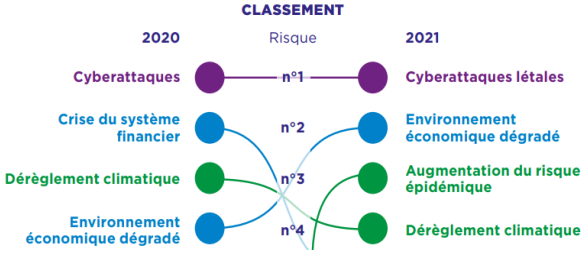
Aujourd'hui, le risque cyber est devenu un sujet incontournable dans une entreprise. De grandes entreprises ont été touchées par des cyberattaques (exemples en Annexe 1), paralysant leurs outils informatiques, menaçant l'activité et altérant leur image. En 2020, l'ANSSI (l'agence nationale de sécurité des systèmes d'information) a relevé une augmentation de 255 % des attaques au rançongiciel dans son périmètre d'intervention, la sphère publique, les grandes entreprises et celles qui sont essentielles pour la sécurité nationale. Les conséquences des cyberattaques sont variées : pertes financières, réputation écornée, destruction du système d'information, etc. En effet, l'entreprise subit une désorganisation liée à la remise en route du système infecté, à la reconstitution des données perdues, à la mobilisation d'une équipe après une attaque et il faut du temps. En 2017, l'entreprise Saint-Gobain a supporté plus de 220 millions d'euros de dommages sur son chiffre d'affaires quand elle fut attaquée.
De plus, le RGPD fait entrer le risque de pertes juridiques liées à des Cyber-attaques dans une nouvelle dimension : Il prévoit en effet des sanctions pécuniaires allant de 20m€ à 4 % du chiffre d'affaires mondial. Avant l'entrée en vigueur du RGPD, les entreprises européennes ne risquaient pas plus de 500 000€ d'amendes. Pour l'entreprise, l'importance de la cybersécurité réside dans la défense de la valeur économique. Les moyens à mettre en œuvre dans la cybersécurité doivent être à la hauteur de l'exposition et les éventuels impacts économiques.

Cette étude a pour objectif de proposer une démarche ERM pour permettre de piloter l'entreprise par certains risques induits par la transformation digitale des services de l'entreprise et en particulier l'accroissement du risque cyber de perte de données à caractère personnel des assurés. Il s'agit de sécuriser la valeur de l'entreprise face à cette transformation tout en tirant profit des opportunités que cette stratégie présente. Pour ce faire, la première partie présentera la cartographie des nouveaux risques associés à la transformation initiée avec un accent particulier sur l'évaluation de certains risques d'un point de vue résultat et solvabilité dans le cadre de l'ORSA. Enfin s'ensuivra une description des actions de pilotage et de maitrise des risques permettant d'accompagner l'entreprise dans ce changement.

II. Contexte et enjeux

Aujourd'hui, le paysage des risques tout entier semble subir de profonds changements sous l'effet de la digitalisation. Le défi consiste alors à trouver un compromis entre les avantages escomptés de la numérisation et les risques inhérents aux nouveaux modèles économiques qu'elle impose.

Ce risque faussement connu a évolué, depuis la sphère purement informatique et technique et avec la prise de conscience croissante de l'impact économique et financier de cette catégorie de risque, le sujet est devenu l'une des problématiques majeures des entreprises comme le témoigne le schéma ci-contre.



Cartographie prospective 2021 des risques de la profession de l'assurance et de la réassurance de la FFA.

L'ACPR a d'ailleurs commenté le fait que la crise que nous traversons montre l'importance du risque informatique et en particulier de la cybersécurité. Le secteur financier demeure le secteur le plus ciblé par les cyberattaques. Le régulateur souligne que « ce risque mérite d'être pleinement pris en compte dans le dispositif général de gestion des risques et clarifie les attributions des organes de gouvernance en matière d'élaboration d'une stratégie IT, de validation d'une politique idoine et de l'allocation de ressources permettant une prise en charge efficiente de ce risque. Les dirigeants effectifs soient responsables de la définition, de la validation, du déploiement et du suivi de cette stratégie au titre de leur responsabilité générale sur la bonne marche de l'entreprise et de la maîtrise des risques. »

Dans le contexte de ce projet, on se mettra dans le cadre d'une entreprise fictive pour des raisons de confidentialité, s'inspirant d'un cas réel sur le marché (les informations confidentielles m'ont été partiellement partagées). Ce groupe d'assurance mixte a une taille moyenne sur le marché français :

Principaux chiffres	
Primes : 6 Md€ **Nombre d'assurés (DCP) : 5.000.000** **Résultat net (part groupe uniquement): 140 M€**	**Fonds propres durs : 3 Md€** **Fonds propres (S2) : 6 Md€** **Total bilan (S2) 40 Md€** **Taux de couverture du SCR : 200%**

Dans son appétence aux risques, il y a plusieurs indicateurs dont celui du niveau de couverture de l'exigence en capital d'au moins 150% validé par le Conseil d'Administration.

Dans sa stratégie de transformation et digitalisation nommé « DigInov », l'assureur a accéléré sa stratégie pour accompagner son développement durant la pandémie et a mis en place un process de souscription en ligne sur plusieurs produits phares de son offre, en auto/moto et multirisque habitation ainsi que sur la santé et l'emprunteur individuelle. Le service de gestion a également été transformé sur ces lignes pour permettre des traitements automatisés. Lors de la souscription et demande de prestations, les clients enregistrent leurs données personnelles en ligne ainsi que leur moyen de paiement ou compte bancaire pour les prélèvements/paiement de prestations. Ces données sont stockées dans un cloud sécurisé (avec un serveur supplémentaire en *backup*) dans un seul et unique SI pour centraliser et uniformiser les données à des fins de ventes croisés entre les différentes activités. Cela a pour objectif de :

- Améliorer la qualité des données récoltées
- Faciliter les futures souscriptions sur des produits complémentaires
- Simplifier les démarches pour les assurés avec transmission automatisée et amélioration de l'efficacité des traitements
- Réduire les risques opérationnels, les taches manuels et les coûts et donc améliorer le résultat
- Allouer les ressources sur des taches à plus forte valeur ajoutée
- Améliorer l'image de la société auprès des clients, des investisseurs et fournisseurs.

Cette nouvelle stratégie induit de nouveaux risques pour l'entreprise que je propose de traiter via une démarche ERM visant à accompagner le changement initié par l'assureur. Dans ce contexte, l'objectif sera de se focaliser sur la famille de risque opérationnel et en particulier le risque cyber de perte de données personnelles des assurés.

III. Démarche ERM

Au sein de l'entreprise, le risque cyber de perte de données personnelles des assurés prend en effet une place importante dans les échanges avec les différentes parties prenantes et une démarche ERM a tout son intérêt afin d'éclairer le management dans le pilotage de la nouvelle stratégie et prendre du recul sur les impacts éventuels.

Le déploiement de la démarche a pour objectif de se focaliser sur les étapes suivantes basées sur le référentiel COSO (Annexe 2)

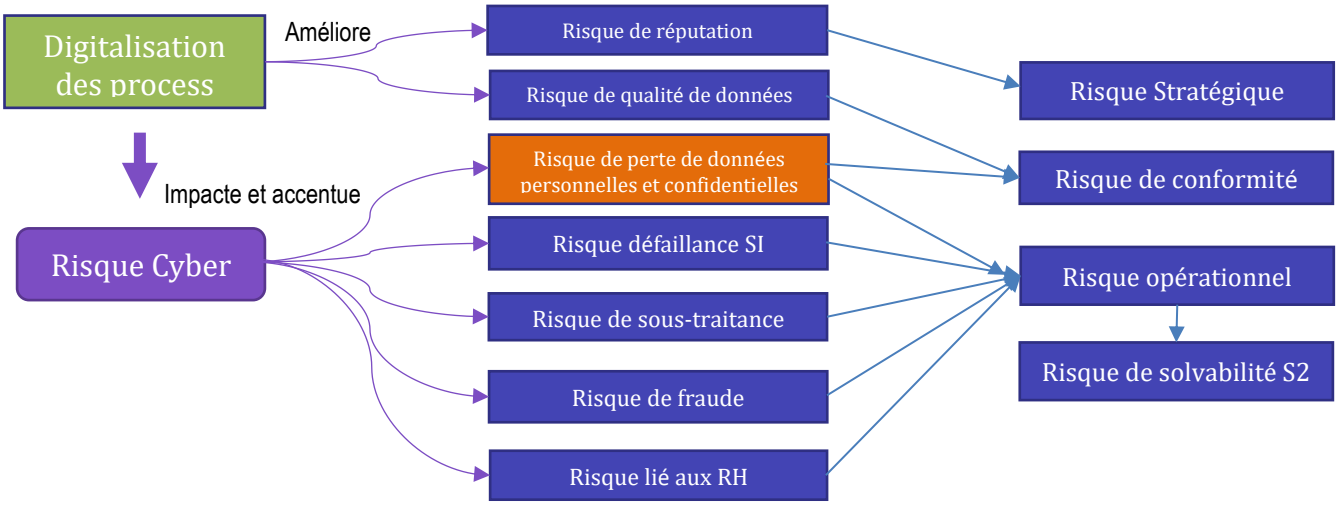
Qui se déclineront selon les actions décrites dans la suite du mémoire

- Une revue de la **cartographie des risques** associée aux impacts du risque cyber
- Description d'**actions de maîtrise et de traitement des** risques permettant de sécuriser la valeur économique de l'entreprise.

3.1 Identification des risques

A partir d'échanges organisés avec différents services d'un client assureur (même caractéristiques de notre cas d'étude), où j'ai déployé avec un membre de la direction des risques un outil d'évaluation basé sur un questionnaire, il a été procédé à l'identification des principaux risques impactés par la mise en place de la stratégie « DigInov » dans l'entreprise, en l'occurrence l'évolution du risque opérationnel et en particulier risque cyber, ce qui a permis de lister les conséquences du risque cyber sur les familles de risques globales. Bien que la nouvelle stratégie ait un impact sur différentes familles de risques (risque technique avec hause éventuelle de la sinistralité par exemple), nous allons nous concentrer sur la famille de risque opérationnel.

Le schéma ci-après permet de mettre en évidence ces différents impacts. Les familles de risques les plus marqués par cette nouvelle stratégie sont développés par la suite.



Les principaux risques liés au risque cyber qui sont induits par la stratégie digitale adoptée par la compagnie ont été listés bien qu'il existe d'autres risques impactés de manière indirecte.

- ***Risque de perte de données personnelles des assurés***

Le déploiement du cloud pour sauvegarder les données à caractère personnel des assurés introduit un risque de cyberattaque avec chiffrement de données et/ou perte/suppression totale des données des assurés qui aura des conséquences importantes en termes de perte d'exploitation suite à un fonctionnement dégradé de l'entreprise le temps de remettre en route les systèmes de secours et de sauvegarde. Cet incident empêchera également de contacter et d'avertir les assurés de l'incident lié à la perte de leurs données et de leurs moyens de paiement pour prendre les mesures nécessaires.

- ***Le risque cyber de défaillance du SI***

Une cyber-attaque peut créer la défaillance du système SI et du cloud interrompant le fonctionnement de la chaine de souscription et de gestion des sinistres ce qui peut engendrait l'incapacité pour l'assureur de régler les prestations dues aux clients et perdre des primes liés aux nouvelles souscriptions non abouties.

- ***Risque de fraude***

Les données des assurés sont centralisées au sein d'un serveur cloud, il est donc possible que le sous-traitant de ce service vole les données des assurés. Une personne en interne avec des accès appropriés peut également voler les données personnelles des assurés avec leurs moyens de paiements.

De plus, la chaine de prestation ayant été automatisée, il est possible que certaines demandes d'indemnisations ne soient plus contrôlées, ce qui présente aussi un risque d'absence de détection de fraude. Ce risque ne sera pas traité dans la suite.

- ***Risque de conformité***

Une cyber-attaque au cloud avec perte de données personnelles y compris données de santé, les moyens de paiements et/ou compte bancaire, introduit le risque de non-conformité au RGPD. De plus, le risque de fraude présenté précédemment augmente le risque de conformité pour non-respect des engagements.

- ***Risque solvabilité***

Le risque de solvabilité est un risque lié à l'évolution du profil du risque opérationnel et cyber en particulier. L'augmentation du risque de non-conformité lié au RGPD et du risque opérationnel avec la nouvelle stratégie digitale a un impact sur le risque de solvabilité. De plus, dans ce contexte, l'ACPR a demandé une prise en compte du risque cyber dans le calcul du BGS dans le cadre de l'ORSA qui peut augmenter le besoin en capital pour l'entreprise dans le futur et remettre en cause son appétence.

- ***Risque de Réputation***

La nouvelle stratégie de l'entreprise va permettre de simplifier les démarches pour les clients et aura pour conséquence d'améliorer l'image de marque de la société.

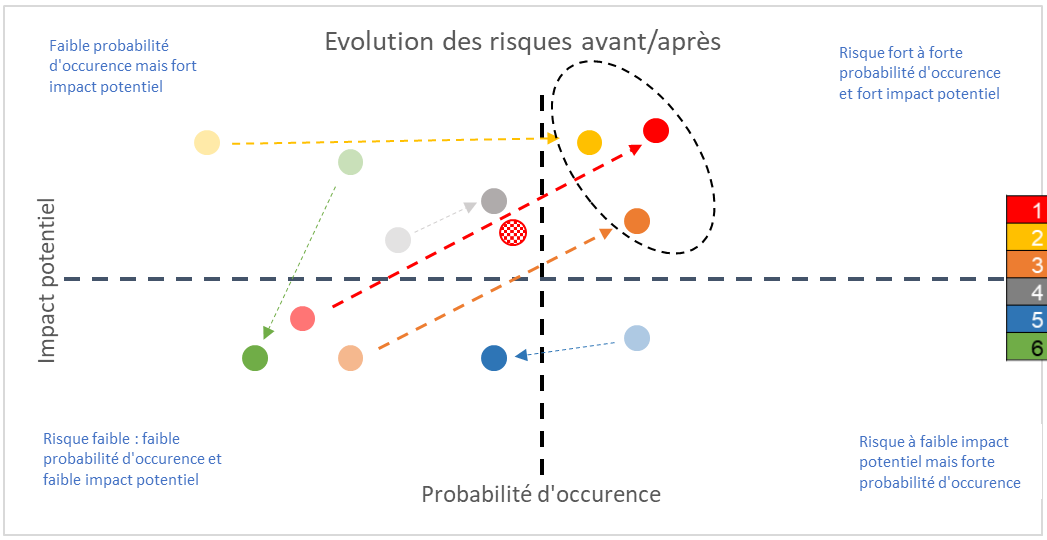
- ***Risque de qualité des données***

Le risque d'erreurs (mauvaise saisie) est diminué grâce au nouveau projet et les échanges automatisés de données. De plus l'uniformisation du système de stockage entre les différents services permet aussi d'avoir des données unifiées et d'améliorer la qualité des données à traiter au sein de l'entreprise pour différents objectifs (indicateurs de pilotage, calculs réglementaire, ventes croisées)

3.2 Evaluation des risques

Les principaux risques de la famille opérationnelle étant identifiés, l'objectif est de les classifier et mesurer leur évolution avant et après la mise en œuvre de la stratégie de digitalisation des services pour pouvoir les prioriser et les traiter. Dans le cadre de l'ERM, il est important d'apporter un éclairage tant quantitatif que qualitatif de l'évaluation des risques de l'entreprise.

Une partie importante des évaluations des risques opérationnels et en particulier risque cyber de perte de données confidentielles est réalisée sur la base de jugement d'experts.



On constate que l'implémentation de « DigInov » a eu des impacts favorables sur les risques de réputation et risque de qualité des données. Le risque de défaillance SI reste contenu et ne présente pas une probabilité d'occurrence plus élevé qu'auparavant, bien que l'impact soit légèrement plus élevé dû à l'exposition plus importante à ce risque.
En revanche, les risques de fraude, conformité et de perte de données confidentielles des assurés deviennent significatifs et nécessitent une attention et un traitement adaptée. Le risque de perte de données a présenté différentes divergences dans son estimation (vs.) ce qui a motivé l'intérêt de rechercher une structure quantitative adaptée pour aider à quantifier ce risque.

3.2.1 Evaluation du risque de perte de Données à Caractère Personnel (DCP)

Certains modèles peuvent être utiles dans l'évaluation du risque cyber de perte DCP. Dans cette section, une méthode de quantification du risque cyber de perte DCP parmi les plus avancées sera présentée. Cette structure de modélisation de sévérité stochastique est issue d'analyse d'études de recherches avancées, présentée de manière succincte en Annexe 3.

- Modèle fréquence/sévérité :

En 2020, Farkas, Lopez et Thomas (Réf 7) ont publié un article qui tend à mesurer les coûts induits par une violation de données à caractère personnel en proposant une amélioration du modèle de Jay Jacobs (Réf 5). L'article se base sur une approche classique d'indépendance entre fréquence et sévérité, permettant d'étudier les deux variables aléatoires séparément et de mieux exploiter l'ensemble des données disponibles. Les études effectuées montrent que le recours aux modèles de régression de Poisson permet de répliquer la fréquence d'occurrence des attaques cyber étudiées de manière satisfaisante. A titre d'exemple, sur les données associées aux entreprises françaises, sous hypothèse d'un modèle de régression de Poisson, la fréquence moyenne d'occurrence (une occurrence correspond à une perte d'au moins 1 DCP) est estimée à 0,42 attaques par an au sein d'une grande entreprise.

De la même façon, il a été motivé et démontré dans l'étude que la variable aléatoire représentant le nombre de données à caractère personnel perdues suit une loi de Pareto Généralisée. Pour rappel, les distributions (GPD) apparaissent naturellement dans l'analyse des variables aléatoires à queues épaisses.

Ainsi, pour un assureur donné, le coût C induit par une violation de DCP peut s'écrire comme suit :

$$C = \sum_{i=1}^{N} f(Y_i)$$

Où N correspond au nombre d'occurrence de violations. Y_i le nombre de DCP perdues
$f(Y_i)$ la valeur du coût induit par la perte de Y_i DCP définie selon la formule de Jay Jacobs:

$$\log\big(f(Y_i)\big) \approx \alpha.\log(Y_i) + \beta \Rightarrow f(Y_i) \approx Y_i^{\alpha}.e^{\beta}$$

Enfin, il est également proposé de recourir à des arbres de régression (Annexe 3) afin d'adapter les paramètres du modèle utilisé aux caractéristiques du risque mesuré. En effet, les arbres de régression tendent à définir des règles permettant de classifier les risques en fonction de certaines caractéristiques en plusieurs groupes au sein desquels sont ajustés différents modèles (dans notre cas, le modèle reste inchangé et seuls les paramètres calibrés changent). Ils sont particulièrement adaptés aux situations où la variété des profils et des caractéristiques du risque peut induire une certaine hétérogénéité dans la mesure de la perte. Cela est d'autant plus vrai dans le cas du risque cyber de perte DCP dont les coûts induits sur les entreprises présentent des disparités (en matière de fréquence et de sévérité).

Notons que les modèles étudiés présentent une limite forte car ils ont été étudiés et calibrés sur la base PRC (Annexe 3), avec un nombre restreint d'incidents d'une part et que la calibration est devenue ancienne au regard du caractère fortement évolutif du risque. A défaut de données existantes fiables, toute calibration et évaluation avec ces modèles devra être éprouvé surtout au vu du caractère évolutif du risque.

Ainsi, à l'aide de cette structure de modèle de sévérité, je propose d'établir une matrice de sévérité de référence faisant le lien entre le nombre de données perdues et le coût. Il sera donc possible d'établir, pour chaque classe définie, des métriques permettant d'identifier la distribution de la sévérité puis différents quantiles pour évaluer le coût de ce risque.

A titre d'illustration, pour 2 modalités, une matrice de référence de sévérité est présentée ci-dessous en fonction du nombre de données personnelles.

	Scénarios et coûts associés selon le quantile	
Quantile	1 million de données CP	3 millions de données CP
10%	7 179	15 762
20,0%	19 634	43 109
30,0%	40 557	89 051
40,0%	75 386	165 522
50,0%	134 561	295 454
60,0%	240 186	527 376
70,0%	446 444	980 256
75,0%	629 274	1 381 697
80,0%	922 233	2 024 945

	Scénarios et coûts associés selon le quantile	
Quantile	1 million de données CP	3 millions de données CP
85,0%	1 439 906	3 161 598
90,0%	2 522 280	5 538 164
95,0%	5 789 436	12 711 852
96,0%	7 374 836	16 192 911
97,0%	9 930 686	21 804 788
98,0%	14 749 044	32 384 448
99,0%	27 511 721	60 407 432
99,5%	48 675 516	106 876 736
99,9%	157 845 363	346 580 750

3.2.2 Ajustement de l'évaluation du SCR opérationnel

Le changement de profil de risque de l'assureur avec l'augmentation du risque opérationnel et de conformité a un impact sur la solvabilité prospective dans le cadre de l'ORSA. Dans cette section, je propose une formulation pour prendre en compte l'incidence du risque opérationnel cyber de perte DCP sur le SCR

Le risque opérationnel correspond à la mesure de l'impact sur l'activité d'incidents opérationnels auxquels l'entreprise peut avoir à faire face, dont la fraude, des incidents informatiques, RH, liés à la conformité, des erreurs de calculs, des incidents Cyber. Ainsi, le SCR opérationnel tend à mesurer les pertes pouvant être induites par le risque étudié. Pour rappel, l'exigence de capital associée au risque opérationnel (détail rappelé en Annexe 4**)**, est définie dans le règlement délégué, comme suit :

$$SCR_{Operationnel} = \min(30\%.BSCR, Op) + 25\%Exp_{UC}$$

Le terme Op est donc calculé sur des quantités représentatives de la taille d'une entreprise qui, pour rappel, est une variable explicative du coût induit par une attaque cyber de type perte de DCP. Néanmoins, afin de tenir compte de ce risque de manière plus adéquate, je propose de revoir le terme Op en introduisant un capital *addon* dont la valeur est déterminée à l'aide du modèle retenu précédemment. Il est proposé d'ajuster la composante *Op* :

$$Op_{ajusté} = max\ (Op_{Premiums}\ ; Op_{Provisions}\ ; Op_{Cyber})$$

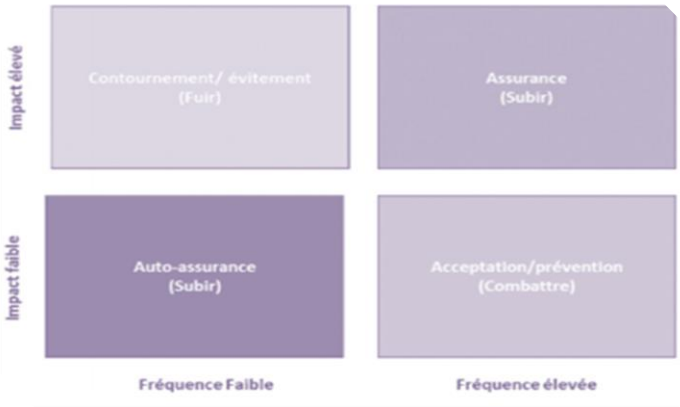
L'estimation du risque opérationnel dans la Formule Standard, *Op*, étant une combinaison linéaire de quantités directement représentatives de la taille d'une entreprise (primes acquises ou provisions techniques), il est possible de s'attendre à observer une relation à peu près proportionnelle entre *OpCyber* et la taille d'une entreprise. Cette proposition d'ajustement proposée est simple et conforme à la fois à la logique de la formule standard et au risque mesuré.

Enfin, le modèle défini dans la partie précédente illustré via la matrice de sévérité ci-dessus, permettrait d'identifier le montant de capital à immobiliser pour faire face à une attaque cyber de type DCP avec une probabilité supérieure à 99,5% et ainsi de mesurer le capital *addon* à considérer. De plus, la matrice précédente serait en effet très utile dans le cadre de l'ORSA et l'évaluation prospective des besoins en capital et de la solvabilité, car elle permettrait de définir des scénarios probables de type Cyber-attaques impliquant des pertes de DCP. D'ailleurs, contrairement au calcul du SCR, il n'est pas nécessaire de se baser sur un niveau de risque de 99,5 %. Des exemples de scénarios ORSA à partir de cette matrice sont illustrés en Annexe 5.

Dans cette section, il s'avère que le risque de perte de données confidentielles d'assurés est le plus significatif dans le périmètre des familles de risques étudiés, nécessitant ainsi la mise en œuvre de dispositifs de maîtrise dédiés.

3.3 Suivi et dispositifs de traitement du risque

Dans cette partie, j'aborderai les actions de maîtrise proposées pour faire face à ces nouveaux risques. Quatre stratégies différentes sont possibles. En effet, selon une approche coût-bénéfice, toute stratégie devrait être bâtie sur le principe d'un coût de gestion du risque ne devant pas excéder la perte potentielle qu'il est censé couvrir.



Les actions de maîtrise à déployer sont :

- La **mise en œuvre d'indicateurs de mesure et de pilotage** permettant le suivi et la maîtrise du risque
- Une **revue des dispositifs de contrôles**
- Le déploiement d'actions
  - De prévention type **formation** et de **communication**, visant à accompagner les collaborateurs à l'émergence de ce risque
  - **D'atténuation** : transfert et/ou couverture

3.3.1 Indicateurs de suivi et de pilotage

Les indicateurs doivent permettre de piloter les risques, de mesurer l'efficacité des plans d'action et d'assurer l'adéquation des moyens aux enjeux et risques auxquels l'entreprise est confrontée. Ils permettent aussi de valoriser le travail des opérationnels, la bonne utilisation des budgets alloués et les éventuels manques en la matière. La mise en place d'indicateurs doit être pragmatique, c'est-à-dire concilier la valeur ajoutée de l'indicateur avec la difficulté d'avoir des données pertinentes (ou qualité trop médiocre) et la charge nécessaire à la fourniture de ces données.

Des indicateurs ont été embarqués dans cette stratégie de digitalisation pour mesurer et évaluer les actions de pilotage en collaboration avec des experts en cybersécurité, la DSI, les services de souscription, de gestion et direction des risques du contrôle interne. J'ai proposé en complément des indicateurs simples à mettre en place et à suivre permettant de mieux piloter les actions de maitrise.
Un premier indicateur qui permet de mesurer le taux de données jugées sensibles dans les bases de données stockés dans le cloud.

$$Taux\ de\ présence\ de\ données\ sensibles\ = \frac{Nombre\ de\ données\ personnelles\ sensibles}{Nombre\ total\ de\ données\ à\ caractère\ personnel}$$

Pour identifier ces données sensibles, une classification devra être réalisée dans la base :

- Données sensibles 1 : Moyens de paiement et compte bancaire
- Données sensibles 2 : Tél, courriel et adresse postale des assurés

En effet, la fuite de ces données est jugée celle présentant l'impact le plus important en termes de conformité et perte d'exploitation (recontacter les assurés, paiements des prestations, remise en route).
Cette classification permettra de décliner les indicateurs suivants :

Taux de présence de données personnels sensibles auprès des clients résiliés

- Pour réduire le risque, **supprimer définitivement les données de paiement et d'adresse postale des clients qui ont résiliés depuis plus de 2 ans** ainsi que les clients qui ont résiliés pour motif d'insatisfaction supérieur à 4/5.
- Il a été **démontré statistiquement** que les clients qui ont résiliés **plus de 2 ans ont moins de 10% de chance** de resouscrire. De même la probabilité de resouscrire dans les 2 ans d'un client insatisfait est très faible. En revanche, le reste a été jugée acceptable et potentiel pour des futurs souscriptions en ligne accélérés via des campagnes marketing ciblées.

Taux d'incidents liés aux données jugées sensibles

- Ce taux permettra de **mesurer la fréquence et la probabilité** que le risque de perte de ces données puisse se produire avec la nouvelle architecture et **mettre ainsi des mesures de détection et prévention adaptées.** Jusqu'ici, le nombre d'incidents globales recensé n'était pas exploitable car il était très hétérogène. Pour mettre en place ce taux, des actions seront réalisées : **recensement et classification des incidents informatiques** par typologie des données pour identifier les incidents liés aux fuites de données personnels sensibles (exemple : dysfonctionnement du site internet où il devient possible d'accéder à l'espace personnel de n'importe quel assuré sans rentrer le mot de passe).
- **Réalisation des tests d'intrusions et stress tests pour mesurer les failles**. Ces tests devront continuellement évoluer pour prendre en compte les dernières approches de cyberattaque et pour éliminer les failles restantes, et aussi pour enrichir la base d'incident.
- **Un seuil a été défini** avec les experts en cybersécurité à partir duquel, l'assureur doit prendre des mesures plus drastiques sur la sécurité du SI et du cloud.

Durée de résolution d'un incident sensible

- Cet indicateur générique a été adaptée au nouveau contexte et permettrait **de piloter et améliorer les** actions à mettre en place lorsqu'un incident majeur de données **sensisbles se produit** et **ainsi limiter le coût d'un risque** de perte de données majeurs dans le futur.

Par ailleurs, pour le risque de conformité, on pourrait aussi envisager de mesurer le taux de réussite du personnel aux formations sur le RGPD et sur la manipulation de données à caractère personnel. Et le taux de réussite aux tests d'intrusion aléatoire (envoi de courriels à certains salariés pour tester la capacité de résistance et résilience des systèmes et du personnel). Ensuite, on définirait un seuil minimal à maintenir.

Seuil minimal critique = taux de réussite de X% du personnel aux formations sur le RGPD

Enfin, il y a également un certain nombre d'indicateurs pertinents (inexistants actuellement) que j'ai proposé de mettre en place pour prévenir et réduire les risques à traiter en priorité, notamment

- ✓ **Taux de sensibilisation** des clients au menaces de *phishing*
  - ➢ Envoie un nombre de mail par semestre aux clients : sensibilisation aux menaces de *phishing*
  - ➢ Réalisation des tests de phishing ciblée : transmis aux clients tagués importants (primes dépassant un certain seuil, informations stockées très sensibles et importantes).
- ✓ **Nombre de failles détectées** classées par niveau d'impact sécurité

3.3.2 Evolution des dispositifs de contrôle

La mise en place d'un dispositif de contrôle constitue un enjeu majeur de sécurisation des activités et de protéger les intérêts de l'entreprise. Ce dispositif se décompose en trois niveaux :

1. **Contrôle permanent de niveau 1** : Réalisé par les opérationnels ou par la hiérarchie
2. **Contrôle permanent de niveau 2 :** Réalisé par des équipes dédiées à ces tâches qui pilotent le dispositif du contrôle permanent. Ces contrôles permettent de s'assurer de la fiabilité des contrôles du niveau 1 mais également de diligenter ses propres contrôles.
3. **Contrôle périodique de niveau 3 :** Audit interne, indépendant, qui évalue la pertinence du dispositif de contrôle global.

La stratégie digitale mise en place aura une incidence sur ces dispositifs de contrôles qui devront s'adapter pour renforcer l'entreprise face aux vulnérabilités d'un point de vue opérationnelle et organisationnelle.

<u>Niveau 1 : Accompagnement des équipes opérationnelles</u>

Les équipes opérationnelles de souscription et de gestion devront s'organiser de manière différente s'inscrivant dans une gouvernance plus adaptée à la stratégie. En effet, les prestations sont quasi automatisées, ainsi les contrôles humains des documents vont disparaitre, ce qui pourrait aboutir à un risque de non-détection des fraudes aux prestations par exemple. De même pour la souscription, il est possible d'avoir des tarifs non adaptés ou accroitre l'antisélection. Par ailleurs, les équipes peuvent avoir accès et à manipuler plusieurs données personnelles des assurés dans des systèmes informatiques nouvellement mis en place. Des adaptations ont été mises en place notamment sur les aspects techniques, que je propose de compléter sur les aspects de gouvernance :

- ➢ **Intervention au point de process sensible** : un contrôle exhaustif par les équipes opérationnels de chaque dossier jugé sensible doit être réalisé.

En effet, pour certains dossiers présentant des informations sensibles et atypiques, le client devra appeler le service souscription/commerciale pour finaliser la souscription ou le service de gestion pour les prestations, qui demandera des documents complémentaires si besoin pour réduire le risque de fraude. Les saisies devront être revues par le responsable de chaque service afin de s'assurer que les informations sensibles ont été saisies dans les champs appropriés et que les données confidentielles inutiles sont bien supprimées. Enfin, à chaque demande de résiliation d'un client dont la prime ou la catégorie SCP jugée sensible, il faut s'assurer que les données personnelles sensibles (médicales, données de paiement) ont également été supprimés. Les indicateurs de données sensibles définis précédemment permettront de réévaluer l'efficacité de ce process.

Pour que les contrôles soient efficaces, des seuils de souscription et de prestations ont été définis et sont actuellement revus pour validation, avec différentes parties prenantes notamment, les responsables métiers, risque, actuariat et IT, en lien avec l'appétence et la tolérance de l'entreprise.

- **Proposition de réaliser un scan périodique des ordinateurs** de collaborateurs manipulant les données sensibles permettant de vérifier si des données de paiement notamment ont été stockés et ainsi relever chaque anomalie dans le journal d'incidents
- **Communiquer auprès des collaborateurs** et parties prenantes des actions mises en place pour une meilleure acculturation du risque et pour maintenir une confiance par rapport aux nouveaux dispositifs.

Niveau 2 : Renforcement et évolution des dispositifs de contrôles

Pour le risque de conformité, l'entreprise a mis en place récemment une nouvelle fonction de vérification de la conformité pour se préserver des risques de réputation et/ou de sanction judiciaire ou administrative, mais aussi pour assurer la protection de ses clients. Cette fonction Vérification de la conformité est une fonction autonome ce qui permet de garantir son indépendance et son impartialité vis-à-vis des opérationnels et renforcer l'efficacité de ses missions.

Par ailleurs, une équipe dédiée a été mise en place pour réaliser des contrôles aléatoires sur des échantillons et ainsi détecter si les mesures opérationnelles mises en place sont adaptées. Cette équipe doit aussi évaluer le contrôle sur les opérations de protection de données mises en place. Je propose **le renforcement de cette équipe par un expert en cybersécurité**, puisque l'équipe actuelle a été composée principalement par des personnes internes métiers et IT, ce qui permettrait d'élargir le champ des compétences et des contrôles.

De plus, je propose **d'étendre les responsabilités du *Chief Data Officer*** rattaché au DG de l'entreprise et qui a pour principal objectif de gérer la stratégie marketing digitale de l'entreprise pour mettre en place une méthodologie permettant l'exploitation des données de façon intelligibles avec les outils de big data, mais n'incluant pas dans son périmètre de stratégie de gouvernance de la donnée, les contraintes et mesures de cyber défense qui relevait plutôt du rôle de la DSI. Au-delà d'assurer la qualité et la fiabilité des données pour tirer profit de cette nouvelle stratégie, les responsabilités devrait inclure à mon sens la protection et la sécurité de la donnée (notamment les données à caractère personnel et données de santé), en particulier pour :

- Organiser la stratégie de collecte de la donnée sensible pour contrôler la limitation des données personnels au sein des services.
- Assurer et organiser l'accès aux données aux personnels formés et sensibilisés
- Assurer la conformité réglementaire des données personnels (RGPD) en collaboration avec la nouvelle fonction de vérification de la conformité
- Définir la politique de la protection de données personnelles avec l'équipe de contrôle dédiée
- Intégrer le dispositif de pilotage de l'entreprise en participant à la définition des scénarios de stress notamment pour l'ORSA et la déclinaison de l'appétence sur la donnée

Niveau 3 : Evolution du contrôle périodique

Dans le plan d'audit actuel, bien qu'il existe un audit des processus de sécurisation des données, l'**audit des sous-traitants** informatiques embarqués dans la nouvelle stratégie de digitalisation n'a pas été intégré, notamment pour les fournisseurs du cloud de stockage des données parce que les contrats en place ne le permettaient pas. Je propose non seulement de faire évoluer les contrats mais surtout, entre temps de faire réaliser **des audits et tests d'intrusion par des tiers** sur les systèmes SI des fournisseurs et faire évoluer les critères de sélection des futurs fournisseurs.

3.3.3 Mesures de prévention et atténuation complémentaires

De plus, des plans opérationnels ont été proposées, en particulier pour le risque cyber de pertes de données sensibles que j'ai complété par les propositions suivantes :

Mesures de prévention et de réduction

- ✓ **Bloquer les accès** à différents sites de transfert et chargement de données (i.e. dropbox) y compris services de courriels personnels
- ✓ **Encoder et chiffrer les données** inactives des assurés résiliés notamment
- ✓ **Tester les accès** des collaborateurs aux données sensibles.

Ainsi que des plans organisationnels complémentaires basés sur des pratiques de marché dans d'autres industries :

- ✓ **Développement de la résilience** « cyber » de l'organisation **par une politique de « chocs » volontaires** (entretenus par exemple par des tests non annoncés, ou par des exercices de simulation).
- ✓ **Renforcement du PCA** en conséquence de la nouvelle stratégie et du plan de reprise d'activité
- ✓ **Documentation en** interne de tous les incidents survenus afin de constituer une base de travail pour enrichir et améliorer la matrice de sévérité de référence et aussi expliciter les pistes d'amélioration
- ✓ **Communication** externe pour assurer les investisseurs et assurés sur les dispositifs de sécurité
- ✓ Mise en place une **politique d'hygiène.** *Guide d'hygiène informatique (ANSSI, 2017)*

Enfin, lorsque la fréquence et l'impact sont tous deux relativement élevés, l'assurance devient la meilleure solution pour la gestion dudit risque.

3.3.4 Mesures de transfert et couverture

Le risque de perte de DCP est un risque de pointe, c'est-à-dire que certains sinistres, peu fréquents, sont susceptibles d'engendrer des coûts importants. Pour ce type de risque, à la fois assez fréquent et avec quelques sinistres pouvant coûter très cher, la mesure de transfert la plus adaptée est la souscription d'une police avec une limite élevée mais avec une franchise assez élevée également afin d'éviter que la prime d'assurance soit trop coûteuse. Il n'y a aucun contrat d'assurance risque cyber pour l'instant et vu les nombres de données en jeu, je recommande la mise en place d'un contrat adapté en calibrant les limites en fonctions des coûts/bénéfices. A titre d'illustration, une analyse a été réalisée avec les données de l'entreprise permettant d'évaluer le bénéfice en fonction du quantile choisie en comparaison avec l'approche sans assurance en Annexe 6 sur la base d'un outil interne.

La mise en place de stratégies de transfert et de couverture adaptées au risque cyber est un enjeu crucial pour les assureurs. La couverture est assurée pour sa grande majorité par le marché de la cyber-assurance. Néanmoins, le manque de données chiffrées, la nature systémique du risque, le défaut de métriques et a fortiori de modèles économiques fiables permettant d'estimer le coût économique des cyber-risques, limitent énormément le développement de contrats d'assurance cyber.

IV. Conclusion

A travers ce mémoire, j'ai proposé une démarche ERM qui a permis de compléter le dispositif de pilotage de l'entreprise en place en réponse aux nouveaux risques issus de la nouvelle stratégie de digitalisation, en particulier le risque de perte de données sensibles des assurés. Cette démarche a permis de :

- **Analyser et identifier les risques** avec les différentes parties prenantes et les opportunités offertes avec cette nouvelle stratégie
- **Classifier, mesurer et prioriser les risques** à traiter, en particulier le risque de perte de DCP en proposant une structure de modélisation de sévérité stochastique issue d'analyse d'étude de recherches, ainsi que par la définition de scénarios dans le pilotage de l'ORSA.
- **Définir des indicateurs d'évaluation et de mesures des actions de maitrise**, en particulier avec la proposition d'indicateurs sur le suivi des taux de données sensibles et leur gestion, aussi par la prise en compte du risque dans l'évaluation et le suivi de la solvabilité prospective pour contrôler le niveau d'appétence définie
- **Adapter les process et traiter le risque** via différentes propositions de revue de gouvernance en place et des solutions de réduction, de transfert permettant d'accompagner l'entreprise

Quelques propositions faites dans ce mémoire n'ont pas été chiffrés, il conviendrait donc de procéder en priorisant les actions présentant le ratio Bénéfice(risque)/Coût le plus élevée afin de maitriser les impacts sur le résultat de l'entreprise.

Ce projet a permis également de tirer des enseignements :

- Les tendances du marché sur le risque cyber et de perte de données sensibles caractérisés dans les grandes entreprises ne doivent pas être interprétées comme des vérités absolues de manière générale et doivent être relativisées pour les entreprises de moyennes/petites tailles.
- Les indicateurs doivent toujours être pratique à mettre en œuvre intégrant le triptyque : 1.Données existantes pour le calcul, 2. Charge pour fournir les données avec une qualité acceptable, 3.et présentant un intérêt pour les parties prenantes. A titre d'illustration, le cas des comptes d'accès laissés actifs après le départ des assurés : ce point clé pour la sécurité ne suscitera pas le réel intérêt d'un directeur financier. Cependant, s'il est possible de valoriser la présence de chaque compte en coût d'abonnement (accès aux outils cloud/plateforme) ou d'exploitation (accès au site Web), nous transformons un problème de sécurité en problème de maitrise des dépenses pour lequel nous devrions avoir toute l'attention de la Direction Financière.
- L'absence de police d'assurance contre le risque cyber de perte de DCP est surtout dû au manque d'offre adaptée sur le marché. Une alternative possible pour se couvrir contre ce risque consiste à transférer le risque aux marchés financiers à travers la titrisation (Annexe 6). En effet, la compagnie d'assurance peut émettre des titres de dettes obligataires par le biais d'une entité juridique. Ces titres sont vendus aux investisseurs et les fonds perçus sont placés sur un compte accessible à l'assureur en cas de réalisation d'une cyber-attaque. En contrepartie, les investisseurs perçoivent un coupon annuel correspondant à la rémunération de leur placement.

Enfin, en s'adaptant au risque cyber, d'autres risques sont créés , notamment le risque humain qui n'a pas été traité dans ce mémoire bien qu'il présente dans cette stratégie une évolution importante : en effet les missions des opérationnelles ont poursuivi leur évolution, passant de tâches administratives vers des missions de contrôle et de contact des clients nécessitant à nouveau le développement de compétences et un accompagnement au changement qui présentent des risques passablement connus et des opportunités pour l'entreprise.

Annexes

Annexe 1 – Typologie et illustration du risque cyber

1. Exemples de risques Cyber

Vol de données de cartes bancaires (2005 à 2007)

En 2007, TJ Maxx, une chaîne de grands magasins opérant principalement aux États-Unis révèle une fuite de données de ses serveurs ayant débuté en 2005 et concernant des transactions remontant à 2003, en particulier des coordonnées de cartes de débit et de crédit liées à des transactions bancaires passées. Les hackers ont opéré de juin 2005 à janvier 2007. Les hackers ont pu voler via une simple connexion Wifi des données de TJ Maxx, mais également de toutes les autres filiales du groupe auquel l'entreprise appartenait : Marshalls, Winners, HomeSense, HomeGoods, . et ce dans plusieurs pays différents (États-Unis, Royaume-Uni, Canada, Irlande). Plus de 100 millions de clients ont été exposés à l'attaque et 46 millions ont été effectivement victimes. TJ Maxx a dû payer des frais administratifs et des remboursements liés à la fraude très conséquents (environ 800 millions $) et s'est fait attaquer en justice lors d'une *class action* menée par une association de banques victimes, ayant dû réémettre un très grand nombre de cartes bancaires à la suite de l'attaque. Il est possible de retenir de cette attaque que TJ Maxx conservait des données de transactions bancaires sur de très longues périodes, que les hackers ont pu voler des données pendant une durée de plus de 18 mois et qu'une intrusion via TJ Maxx permettait de récupérer des données issues d'autres filiales du groupe et des transactions issues d'autres régions du monde.

Saint-Gobain (2017)

En juin 2017, le groupe multiséculaire Saint-Gobain est victime du rançongiciel NotPetya, ce dernier s'étant infiltré dans son réseau interne via sa filiale ukrainienne. L'infiltration provient d'un logiciel du site de l'administration fiscale ukrainienne ayant infecté la filiale de Saint-Gobain. Plusieurs systèmes d'information ont été bloqués à la suite d'un chiffrement par le virus, immédiatement suivi par la suppression massive de données, en à peine quelques minutes. De fait, les réseaux de distribution du groupe ont dû revenir temporairement au crayon et au papier pour la gestion des commandes. L'activité n'a été perturbée qu'une dizaine de jours mais pourtant, les pertes pour Saint-Gobain ont été considérables et estimées à plus de 220 millions d'euros de chiffres d'affaires.

Ces 2 exemples illustrent les 2 types de Cyber-attaques les plus impactantes : la perte de données (TJ Maxx) et la Cyber-extorsion (Saint Gobain). De plus, la chronologie de ces attaques permet de se rendre compte de la prise de conscience du risque Cyber et des politiques de sécurité informatique au cours des décennies : inexistantes dans les années 80, balbutiantes dans les années 2000 puis au cœur de la stratégie de l'entreprise illustré par Saint Gobain et sa politique de sécurité mise en place *a posteriori* de l'attaque.

2. Les types de Cyber-attaques

Exfiltration de données : Une attaque de type exfiltration de données a pour objectif de récupérer des données confidentielles, le plus souvent cela concerne des données personnelles conservées par des entreprises mais cela concerne également des données professionnelles confidentielles. Les catégories de données pouvant être volées sont :

- **Données d'Identité Personnelles**, telles que le nom complet, les détails de contact (adresse physique, adresse courriel, date de naissance, numéro de passeport ou de permis de conduite, numéro de sécurité sociale).
- **Données de carte bancaire**, en complément des données d'identité personnelles, telle que le numéro ou l'empreinte de carte bancaire de débit ou de crédit, code PIN, RIB, code d'accès aux services bancaires.
- **Données médicales**, en complément des données d'identité personnelles, des données concernant une pathologie, une posologie, des rendez-vous pris avec des experts médicaux ou des données relatives à des opérations de santé, des identifiants biométriques (empreintes digitales, d'iris), des résultats de tests médicaux.
- **Données professionnelles confidentielles** : informations sensibles liées à des propriétés d'entreprises, de secrets industriels, d'informations confidentielles au sujet de contreparties.
- **Données de propriété intellectuelle** : brevets, croquis industriels, recettes de fabrication.

La sévérité d'une attaque de type exfiltration de données est fortement corrélée au nombre de données perdues (pour les données personnelles), ainsi qu'au type de données et donc implicitement à la taille et au secteur d'activité de l'entreprise attaquée. Les causes peuvent être accidentelles (perte d'un ordinateur professionnel avec accès au réseau de l'entreprise par exemple), malveillantes externes ou malveillantes internes.

Pertes de données : l'attaque de type perte de données vise à effacer, de manière temporaire ou définitive, des données d'une entreprise. L'auteur est moins susceptible de tirer profit de son attaque, mais l'entreprise victime peut subir des pertes très importantes, notamment à cause d'une interruption d'activité.

Attaque par déni de service : l'attaque de type déni de service 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, par exemple la mise hors service d'un élément de production physique d'une entreprise via la mise hors service de son système informatique.

Cyber-extorsion : 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. Le principal type d'attaques de Cyber-extorsion est le rançongiciel, consistant à infecter une machine (un ordinateur personnel le plus souvent) et, dans un premier temps, à crypter les données présentes sur la machine de manière imperceptible pour la victime puis dans un second à bloquer la machine en proposant simultanément à la victime de payer une rançon afin de débloquer la machine et décrypter les données. Les montants ne dépassent généralement pas quelques centaines d'euros ou de dollars US, et sont le plus souvent exigés en crypto-monnaies (e.g. Bitcoin).

Annexe 2 : Référentiel COSO

Le COSO est un **référentiel de gestion des risques** existant depuis 1992 et défini par le *Committee Of Sponsoring Organizations of the Treadway Commission*.

En 2017, une nouvelle édition de ce référentiel a été publiée, visant à refléter de nouveaux enjeux (transformations majeures tirées par la technologie, nouvelles menaces, complexité des environnements économiques) et à intégrer l'évolution des pratiques (notamment, une transparence accrue).

Ce nouveau référentiel souligne en particulier que la maîtrise des risques doit être une **démarche intégrée au cycle de management et de pilotage** de l'organisation.

Référentiel COSO 2017				
1	2	3	4	5
Gouvernance et culture	**Stratégie et définition des objectifs**	**Performance**	**Revue et amendement**	**Information, communication reporting**
Mettre en œuvre une gouvernance des risques et une culture des risques. *Attirer, développer les compétences.*	*Analyser le contexte économique.* *Définir l'appétence aux risques, la stratégie et les objectifs.*	*Identifier, évaluer et classifier les risques.* *Mettre en œuvre les dispositifs de maîtrise.*	*Identifier les évolutions* *Suivre la mise en œuvre, actualiser les cartographies.*	*Automatiser le reporting des risques.* *Communiquer.*

Annexe 3 : Modélisation du risque cyber : perte de données à caractère personnel

La modélisation du risque cyber est un sujet très complexe du fait du manque de données fiables et la rapidité avec lequel ce risque évolue. L'objectif de cette partie et de faire un état de l'art des modèles existants et d'en tirer des conclusions sur le modèle le plus approprié pour évaluer le risque de perte DCP dans le cadre de sa gestion. Une analyse sur les données démontre les limites des modèles et de leur utilisation. *« All models are wrong, but some are useful » - George Box* .

Evaluation du risque cyber (perte de DCP) :

La modélisation du risque cyber représente un véritable défi pour les assureurs, en raison de sa nature mouvante, du facteur humain et d'un manque de données. L'objectif de cette partie sera de faire un état des lieux succinct des méthodes d'évaluation du risque cyber.
Dans un premier temps, nous étudierons la pertinence d'une modélisation directe du coût induit par une cyber attaque de type perte de données à caractère personnel (ci-après « DCP »), en fonction des caractéristiques propres à une entreprise ou encore en fonction du nombre de DCP perdues. Puis, dans un second temps, nous mettrons en avant l'intérêt d'adopter une approche basée sur la fréquence/sévérité afin de mesurer les coûts induits par ces violations.

Modèle à estimation directe du coût

L'institut Ponemon (Réf 3 et 4) (*Ponemon Insitute LLC*) est un centre de recherche fondé par Larry Ponemon dédié à l'étude de la protection des données. Depuis l'année 2006, l'institut publie annuellement, sur la base d'informations collectées auprès d'entreprises, des études qui visent à quantifier le coût des violations de données dont elles ont été les victimes.
Les rapports publiés permettent de mieux appréhender le risque cyber et d'identifier plusieurs variables explicatives du coût induit par les cyber-attaques de type perte de données sur les entreprises. Parmi celles-ci, nous pouvons citer :

- le pays ou la région
- le secteur d'activité
- la taille de l'entreprise

Les données publiées par l'institut *Ponemon* permettent de calculer des moyennes d'indicateurs à différentes échelles (pays, secteurs d'activité et tailles de l'entreprise) et des ajustements proportionnels dépendant du profil de risque de l'entreprise considérée peuvent être réalisés afin de modéliser de manière simple ce risque cyber.

Pays/Région	Coût unitaire	Nombre de DCP perdues
ETATS-UNIS	242 $	32 434
FRANCE	163 $	26 300
ROYAUME-UNI	155 $	23 636
ITALIE	146 $	24 577
ALLEMAGNE	193 $	25 610

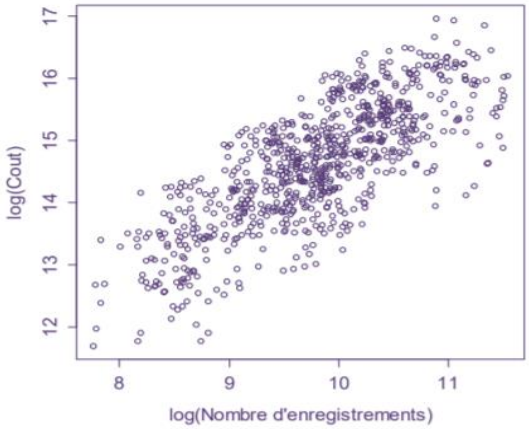
On peut, par exemple, envisager que le coût peut être modélisé comme suit :

$$Cout_{Total} = Cout_{unit}^{pays,secteur} * NB^{DCP} + Ajust^{taille}$$

Néanmoins, cette méthode ne tient pas compte de la distribution des pertes et ne permet donc pas de mesurer et de prédire le risque de manière précise. En revanche, dans une démarche plus pragmatique, il peut être tout à fait possible d'utiliser cette démarche simplifiée pour avoir une idée de l'évaluation du risque. En revanche, pour des entreprises de très grande taille avec des expositions importantes, il est plus pertinent de proposer des estimations basées sur des observations extrêmes.

En 2014, Jay Jacobs a remis en question le lien de proportionnalité entre le coût d'un sinistre et le nombre de DCP. En effet, il a conservé le nombre de DCP comme variable explicative mais a essayé de mesurer la pertinence d'autres formes de modèles.
Il a donc enrichi l'approche précédente et a abouti à un log-log modèle, dont les paramètres sont estimés par régression linéaire, et qui est défini comme suit :

$$\log(coût) = \alpha \log(nb\ DCP\ perdues) + \beta + \epsilon \qquad \text{où } (\alpha, \beta) \in \boldsymbol{R}\ et\ \epsilon \sim N(0, \sigma)$$



Le graphique précédent tend à montrer que le lien de linéarité entre les deux variables considérées semble plausible, néanmoins, les indicateurs statistiques montrent que le nombre de données volées est un paramètre pertinent mais qui n'explique toutefois pas la totalité du coût induit pour les entreprises.
Les résultats induits donc par ce modèle ne sont pas satisfaisants mais permettent d'améliorer de manière notable les résultats obtenus via l'approche précédente.
Finalement, l'étude de la relation directe entre le coût et les variables explicatives choisies permet de confirmer le caractère approprié de ces variables mais ne permet pas d'aboutir à un modèle de prédiction satisfaisant. Toutefois, il apparaît indéniable que l'utilisation d'un log-log modèle basé sur le nombre de données perdues permet d'aboutir à des résultats de meilleure qualité.

Ainsi, le pouvoir prédictif des modèles construits ayant été jugé insuffisant, une modélisation de deux modalités :

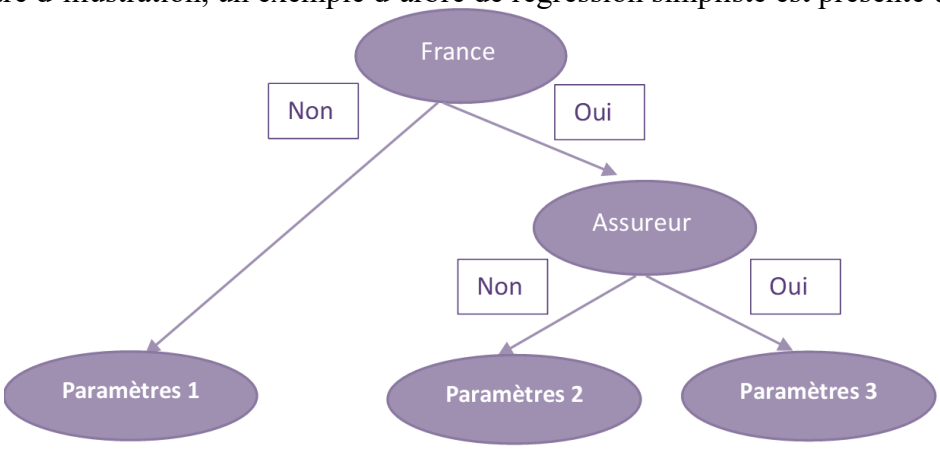
1- Estimation de la fréquence
2- Estimation du coût induit par la perte de données

Est une alternative plus appropriée notamment utilisé l'étude [Farkas , Lopez, Thomas] (Réf .7)

Modèle fréquence/sévérité avec arbres de régression

Enfin, l'article de Farkas, Lopez et Thomas (Réf .7) propose également de recourir à des arbres de régression afin d'adapter les paramètres du modèle utilisé aux caractéristiques du risque mesuré. En effet, les arbres de régression tendent à définir des règles permettant de classifier les risques en fonction de certaines caractéristiques en plusieurs groupes au sein desquels sont ajustés différents modèles (dans notre cas, le modèle reste inchangé et seuls les paramètres calibrés changent). Ils sont particulièrement adaptés aux situations où la variété des profils et des caractéristiques du risque peut induire une certaine hétérogénéité dans la mesure de la perte. Cela est d'autant plus vrai dans le cas du risque cyber dont les coûts induits sur les entreprises présentent des disparités notables (en matière de fréquence et de sévérité).

A titre d'illustration, un exemple d'arbre de régression simpliste est présenté ci-dessous :



Modélisation de la fréquence

L'étude Ponemon

Ponemon estime la probabilité à 29,6% de subir une attaque mettant en cause au moins 10 000 DCP à horizon deux ans (1.8), ce qui correspond, sous l'hypothèse du fréquence qui suit une loi de Poisson, à une espérance de 0,175 attaques par an et par entreprise.
Plus précisément, cette donnée issue de l'étude Ponemon représente la probabilité de subir une nouvelle attaque dans les deux ans, et est estimée à partir de l'échantillon d'environ 500 entreprises sélectionnées pour l'étude qui ont toutes subies des attaques entre Avril 2018 et Juillet 2019. Ce sont majoritairement des grandes entreprises (> 250 employés).

L'échantillon de Ponemon est un ensemble d'entreprises réparties dans le monde entier. A partir de la donnée de 29,6% associée au seuil de 10 000 DCP, et sous l'hypothèse de la loi de Weibull tronquée pour modéliser le nombre de DCP perdues, il est possible d'estimer la fréquence au seuil de 500 DCP.

CESIN (Réf 8)

Le CESIN, ou Club des Experts de la Sécurité de L'information et du Numérique a réalisé un « Sondage OpinionWay pour le CESIN » puis publié son baromètre de la Cyber-sécurité des entreprises en Janvier 2019.
L'enquête a été réalisée auprès des membres du CESIN : https://www.cesin.fr/membres.html
Le CESIN a publié que 80% des entreprises ayant répondu ont constaté au moins une Cyber-attaque au cours des 12 derniers mois. Le chiffre de 80% correspond à une espérance de 1,61 attaques par an sous l'hypothèse d'une loi de Poisson.

Chiffres du CESIN permettant de déduire des fréquences d'occurrence de Cyber-attaques exposant les données d'une entreprise

Type	Probabilité de subir au moins 1 attaque	Espérance de fréquence	Perte de données
Toutes attaques confondues	80%	1,61	NA
Shadow IT	64%	1,02	0
Vulnérabilités résiduelles	52%	0,73	0
Erreur de manipulation	42%	0,54	0
Connexion de postes non approuvés	33%	0,40	0
Exp. de données sur un système d'un presta.	32%	0,39	1
M à j. logicielle - des altérations de d.	26%	0,30	1
Extraction/traitement non approuvés	26%	0,30	1
Dépendance humaine à un système strat.	23%	0,26	0
Action abusive d'un administrateur	21%	0,24	0
Non-suppr. à la fin de contrat avec un presta.	16%	0,17	1
Fraude interne	15%	0,16	0
Malveillance d'un employé	12%	0,13	0
Malveillance d'un prestataire	7%	0,07	0
Non-rest. de d. - changement de presta.	6%	0,06	1
Vente ou cession de données non-autorisées	2%	0,02	1

Utilisation des données CESIN pour l'estimation d'une espérance de fréquence annuelle (1/2)

Périmètre	Espérance de fréquence
Total (somme des espérances de tous les types d'attaques)	4,81
Total - pertes de données uniquement	1,24
Ajustement du total - nb moyen de cases cochées par attaque	2,99
Perte de données ajustée	0,42

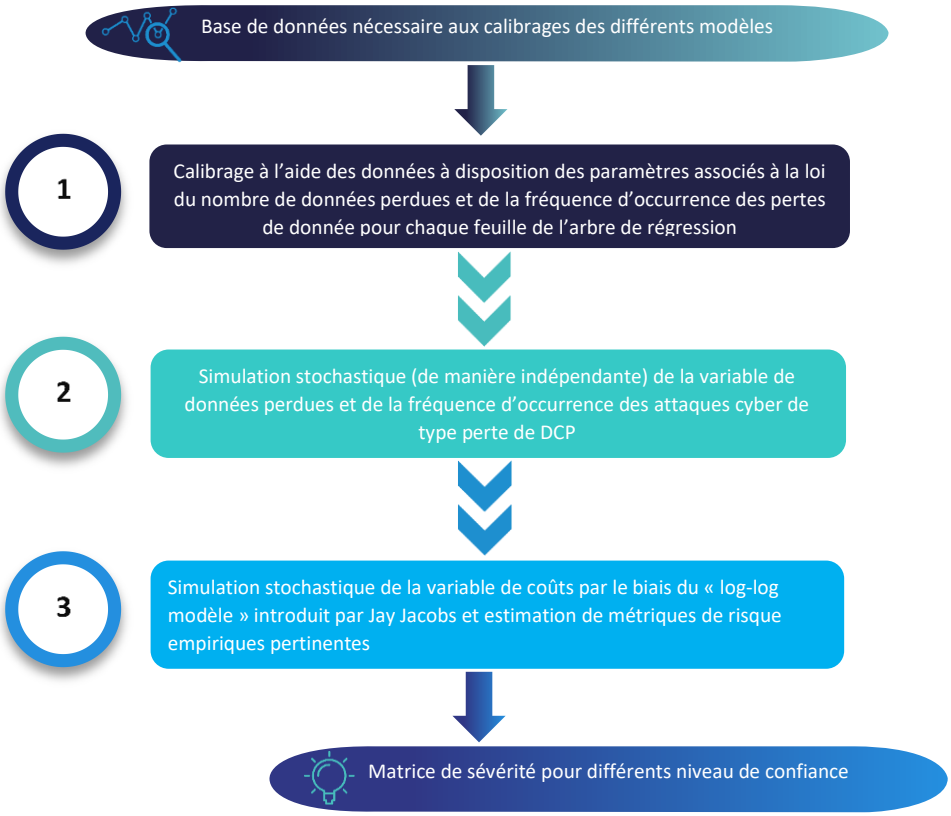
Utilisation des données CESIN pour l'estimation d'une espérance de fréquence annuelle (2/2)

Pour estimer une espérance de fréquence annuelle de subir une attaque de perte de données, les étapes suivantes sont effectuées :

- L'hypothèse que la loi de Poisson est applicable à tous les types d'attaques est retenue.
- L'espérance de fréquence est calculée au total (1,61) et pour chaque risque Cyber (colonne *Espérance de fréquence*).
- La somme des espérances des fréquences pour les attaques susceptibles d'engen- drer des pertes de données est reportée (1,24).
- En supposant que les répondants ont coché plusieurs cases pour chaque attaque effectivement subie, il est possible de déduire que 2,99 cases ont été cochées par attaque subie.
- C'est le rapport entre l'espérance toutes attaques confondues (1,61), et la somme des espérances de toutes les catégories d'attaques (4,81).
- L'espérance de fréquence « perte de données » est ajustée du facteur 2,99.

La loi de fréquence retenue est une loi de Poisson de paramètre 0, 42.

La structure complète du modèle est présentée ci-dessous :



Données

Il existe deux bases de données publiques et gratuites recensant des évènements de types Cyber-attaques essentiellement des incidents ayant eu lieu aux Etats-Unis. Les bases PRC (Privacy Rights ClearingHouse) et VERIS.

- La base PRC contient environ 9000 incidents récences via différentes sources (agences gouvernementales, médias et ONG) avec 13 colonnes interprétables et son utilisation est assez simple et facile d'accès et disponible sur le site de l'association *Privacy Rights* https://privacyrights.org/about. C'est une association à but non lucratif fondée en 1992 ayant l'ambition de protéger la vie privée des citoyens états-uniens en fournissant des informations concernant les droits des individus ainsi que des moyens de défendre leurs droits.
- La base *VERIS Community Database* ou VCDB est une base collaborative reportant des incidents de sécurité et respectant un reporting standardisé : VERIS (Vocabulary for Event Recording and Incident Sharing) et disponible à cette adresse http://veriscommunity.net. Les données proviennent des 2 sources : le *Department of Health and Human Services (HHS)* qui est une organisation fédérale états-unienne, et des différents outils mis à la disposition du public par le *State Attorney General (SAG)* (ou procureur général d'État) de chacun des états américains et informations issues des médias. La collecte d'information dans la base VCDB a débuté en 2013 et se concentre exclusivement sur les incidents de type perte de données (Data breaches)

Ainsi les différentes sources sont presque exclusivement états-uniennes. Les incidents reportés sont issus d'informations fédérales (environ 50%), étatiques ou des médias. De plus, il existe un biais conséquent de telle sorte que les incidents liés au secteur de la santé sont sur-représentés notamment dans la base VERIS.

Annexe 4 : Rappel calcul sous S2 du SCR opérationnel

Le risque opérationnel correspond à la mesure de l'impact sur l'activité d'incidents opérationnels auxquels l'entreprise peut avoir à faire face, dont la fraude, des incidents informatiques, RH, liés à la conformité, des erreurs de calculs, des incidents Cyber.

Dans le cadre du calcul de l'exigence réglementaire de la réglementation Solvabilité 2, le règlement délégué 2015/35, article 104, exige des compagnies européennes d'estimer le risque opérationnel selon la formule :

$$SCR_{Oprationnel} = min\,(0,3 \cdot BSCR\,;\,Op) + 0,25 \cdot Exp_{UI}$$

Avec *BSCR* pour désigner le capital de solvabilité requis de base, *Op* pour désigner le capital requis de base pour risque opérationnel et Exp_{UI} pour désigner le montant des dépenses encourues au cours des 12 derniers mois en ce qui concerne les contrats d'assurance vie où le risque d'investissement est supporté par les preneurs.

Op s'écrit comme :

$$Op = max\,(Op_{Premiums}\,;\,Op_{Provisions})$$

Où : $Op_{P\ remiums}$ et $Op_{P\ rovisions}$ désignent le capital requis pour risque opérationnel sur base respectivement des primes acquises et des provisions techniques.

La composante $Op_{\ Premiums}$ est calculée comme la somme de 4 % du montant des primes pour les engagements d'assurance et de réassurance vie au cours des 12 derniers mois, sans déduction des primes des contrats de réassurance mais avec déduction des primes pour lesquels le risque est porté par l'assuré et 3 % des primes pour les engagements d'assurance et de réassurance non-vie au cours des 12 derniers mois.

De plus, en cas d'augmentation de plus de 20 % du montant de primes acquises tant en vie qu'en non-vie par rapport à l'année précédente, la contribution au calcul des primes acquises (tant en vie qu'en non-vie) au cours des derniers 12 mois supérieures aux primes acquises au cours des 12 mois précédant les 12 derniers mois augmentés de 20 % est doublée.

La composante $Op_{\ Provisions}$ est la somme de 0,45 % des provisions techniques pour les engagements d'assurance vie et de réassurance vie dont sont déduites les provisions pour les engagements dont le risque est porté par l'assuré, et de 3 % des provisions techniques d'engagements d'assurance et de réassurance non-vie.

Annexe 5 : Exemple de scénarios central et stressé définis dans le cadre de l'ORSA

L'évaluation de risque de perte de DCP via la structure présentée peut être étendu dans le cadre de l'ORSA où l'objectif est de proposer des scénarios réalistes et probables d'occurrence d'incidents à l'horizon du plan. Étant donné l'incertitude faible sur le nombre d'incidents, l'évaluation portera essentiellement sur la sévérité. Ci-dessous 2 propositions de scénario dans le cadre de l'ORSA.

Scénario Central :

On estime à 3 millions le nombre d'assurés sur les lignes d'activité transformé dans le cadre de « DigInov » et dont les données transitent par le nouveau système en ligne basé sur le cloud. Pour le scénario central, l'hypothèse est faite que l'assureur doit faire face à un incident impliquant des pertes de données au cours de l'horizon du plan. L'incident est lié à un dysfonctionnement du site internet de l'assureur. Il devient possible d'accéder à l'espace personnel 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 et ces informations bancaires. Le dysfonctionnement est signalé par un particulier directement au service client de l'assureur, surpris du dysfonctionnement. Près de 2 000 000 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 300 000 € pour l'audit du site et 1 000 000€ de perte d'exploitation pour les 24h d'indisponibilité du site internet. Des frais annexes (81 697 €) sont engagés pour la mise en place d'actions correctives et le signalement de l'incident aux autorités compétentes.

Année de projection	1	2	3	4	5
Nombre d'incidents	0	0	1	0	1
Nombre de données			**3 000 000**		
Quantile de perte			**75%**		
Coût en $			**1 381 697€**		

Scénario Stressé :

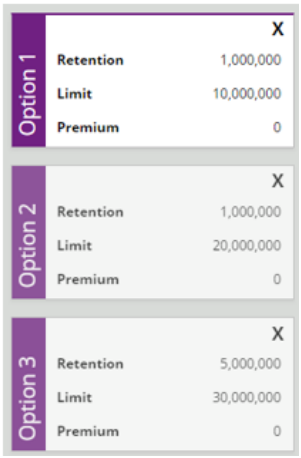
Dans le scénario stressé, le même incident est pris en compte et est modifié : l'hypothèse que le dysfonctionnement remarqué par le particulier n'est pas signalé directement au service client mais est partagé sur un réseau social est retenue. Le service IT ne coupe le site internet qu'au bout de 12h, et plusieurs milliers d'assurés voient leurs données personnelles récupérées par une organisation malveillante. La réputation de l'assureur est largement entachée, l'affaire étant abondamment relayée dans les médias. Un procès est mené contre l'assureur par une association de consommateurs, assortie d'une amende de 0,6 % du chiffre d'affaire de l'assureur suite à une violation du RGPD.

L'assureur estime ses pertes à 1.5M € de perte d'exploitation l'année en réalisant un audit, en bloquant le site et en remettant en route le site de manière sécurisé, 500 000 € suite au procès de l'association de consommateurs, 30M€ d'amende RPGD, et 384 448 € de frais annexes.

Année de projection	1	2	3	4	5
Nombre d'incidents	0	0	1	0	0
Nombre de données			**3 000 000**		
Quantile de perte			98%		
Coût en €			**32 384 448 €**		

Annexe 6 : Illustration de transfert en assurance et de couverture titrisation

Schéma et tableau d'analyse des options de cyber assurance

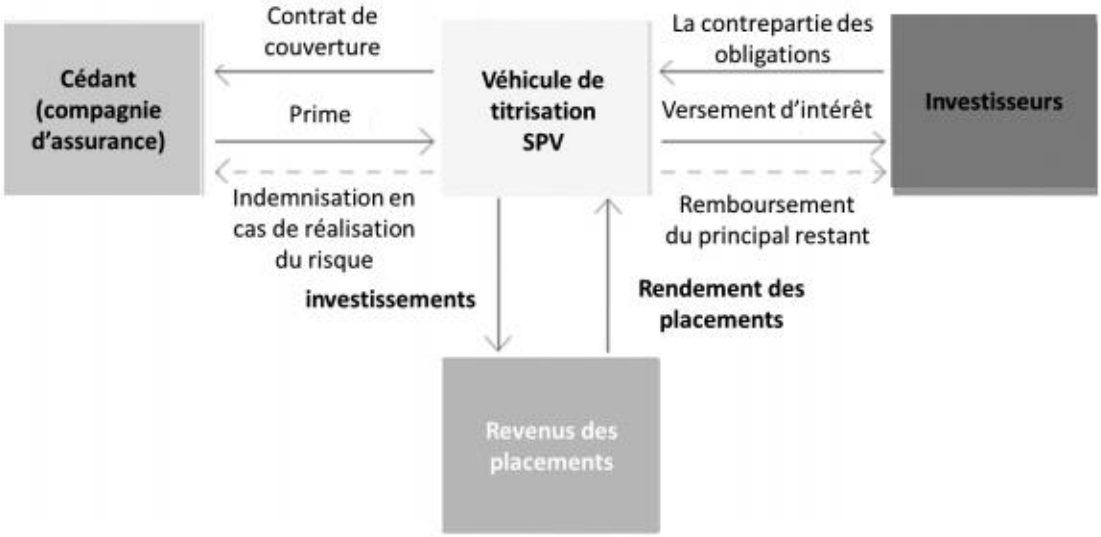


Retained

	Self Insured	Option 1	Option 2	Option 3
Averages	1,025,930	596,791	510,139	588,318
75th Percentile	826,514	627,560	627,240	627,203
90th Percentile	2,204,287	1,110,553	1,074,979	1,607,709
95th Percentile	3,832,379	1,659,748	1,659,748	2,200,800
99th Percentile	13,590,252	4,046,032	2,576,671	5,000,000
99.5th Percentile	25,292,517	15,292,517	5,292,517	5,315,594
99.9th Percentile	54,667,898	44,667,898	34,667,898	24,667,898

Couverture en titrisation

La couverture titrisation consiste à transférer le risque aux marchés financiers à travers la titrisation (ci-après « ILS »). En effet, la compagnie d'assurance cherchant à se couvrir peut émettre des titres de dettes obligataires par le biais d'une entité juridique ad hoc (*special purpose vehicle*) et avec le soutien d'une banque d'affaires. Ces titres sont vendus aux investisseurs et les fonds perçus sont placés sur un compte accessible à l'assureur en cas de réalisation d'un attaque cyber. En contrepartie, les investisseurs perçoivent un coupon annuel correspondant à la rémunération de leur placement assorti d'une prime de risque. D'un point de vue systémique il est donc bien plus sûr de diluer ce risque de pointe chez un nombre important d'investisseurs que de le concentrer massivement chez quelques assureurs potentiellement surexposés en cas d'attaques de grandes ampleurs.



Bibliographie

1. [Verizon, 2015] Verizon (2015) – Data breach investigations report
2. [FFA, 2021] FFA (2021). Baromètre 2021 des risques émergents.
3. [Ponemon et IBM, 2019] PONEMON et IBM (2019) Global cost of a data breach report
4. [Ponemon et IBM, 2018] PONEMON et IBM (2018) Global cost of a data breach report
5. [Jacobs, 2014] JACOBS, J. (2014). Analyzing ponemon cost of data breach
6. [Bessy-Roland et Boumezoued, 2019] BESSY – ROLAND et BOUMEZOUED, A. (2019) Modélisation stochastique individuelle de sinistres cyber.
7. [Sébastien Farkas, Olivier Lopez, Maud Thomas] 2021, Cyber claim analysis through Generalized Pareto Regression Trees with applications to insurance
8. [CESIN, 2019] CESIN (2019). Baromètre de la cybersécurité des entreprises.
9. Guide d'hygiène informatique (ANSSI, 2017), ou le cadre *COBIT 5 Framework* (ISACA, 2016)26.