ACTUARIAL COLLOQUIUM PARIS 2020

La société face au risque Cyber

Emmanuelle Huguet

Thomas Bastard

addactis
THE RISKTECH FOR INSURANCE

Intervenants

ACTUARIAL COLLOQUIUM PARIS 2020

Emmanuelle Huguet

- Senior Manager

Thomas Bastard

- Consultant

addactis

THE RISKTECH FOR INSURANCE

SOMMAIRE

addactis
THE RISKTECH FOR INSURANCE

01 Une dynamique favorable aux attaques Cyber

Une dynamique favorable aux attaques Cyber

Le baromètre 2019

Etude quantitative réalisée par OpinionWay auprès de 174 membres du CESIN en Novembre 2018 interrogés sur internet révèle des chiffres inquiétants :

80%
des entreprises ont constaté au moins 1 fois une cyber attaque

Dont 48%
Ont subi au moins **4 cyberattaques** sur les **12 derniers mois**

41%
des entreprises déclarent être prêtes à gérer une cyber-attaque de grande ampleur

« Les actifs intangibles sont au cœur de l'entreprise »

60 à 90 %
de la valeur d'une entreprise

Un contexte économique favorable aux attaques

- Pression concurrentielle
- La sécurité, en général, pas un argument de vente très attractif
- Editeurs de logiciels et fabricants d'objets connectés ne subissent pas directement les conséquences des failles de sécurité de leurs produits

addactis
THE RISKTECH FOR INSURANCE

Une dynamique favorable aux attaques Cyber

La digitalisation : le changement est la seule constante

" La 5G une véritable rupture technologique "

Véhicules autonomes interconnectés

A horizon **2022**, **500 objets connectés** par foyer

Clés et **mots de passe** remplacés par des **scanners d'empreintes digitales ou de la rétine**

En **2024**, plus que **9%** de transaction en **argent liquide**

addactis
THE RISKTECH FOR INSURANCE

Une dynamique favorable aux attaques Cyber

Une professionnalisation des attaquants (1/2)

Les attaquants jouissent d'une relative impunité

Absence de frontières et différences entre les réglementations nationales

Très complexe d'identifier avec certitude les criminels.

Exemples de types d'attaques organisées marquants

L'espionnage industriel

Affaire Boeing/ Airbus
Condamnation de Boeing à 615 m$

Le sabotage

Les dernières élections américaines

Les attaques de type rançongiciel et hameçonnage

Les mafias font des cyberattaques, peu coûteuses et qui rapportent gros

addactis
THE RISKTECH FOR INSURANCE

Une dynamique favorable aux attaques Cyber

Une professionnalisation des attaquants (2/2)

✓ 5G inattaquable ? C'est faux !

Des risques pour les voitures autonomes

- **Un impact potentiel sur la vie humaine**

Des risques dans l'Internet des objets

- **Multiplication du nombre de failles potentielles**

Des risques pour les sites industriels

- **En raison de nombreux dispositifs électroniques**

✓ Qui est attaqué ? Tout le monde

Les hackers ciblent aujourd'hui en priorité le maillon le plus faible de la chaîne sécuritaire : **l'humain**.

✓ Aucune organisation n'est à l'abri

AIRBUS, City of Baltimore, CHU Rouen Normandie, M6, ICANN, GRAND COGNAC, eurofins, ALTRAN, Edenred, WikiLeaks

addactis
THE RISKTECH FOR INSURANCE

02 Les enjeux réglementaires et assurantiels face au risque Cyber

Les enjeux réglementaires et assurantiels face au risque Cyber

Le risque cyber remet en cause les équilibres existants

Au même rang que les catastrophes naturelles et les pandémies, le risque Cyber un des plus appréhendés chez les acteurs du Marché de l'assurance

Risque potentiellement systémique

Mise en place de groupements ou d'autres structures avec garantie de l'État ?

La question n'est pas de savoir si on va être attaqué mais bel et bien quand !

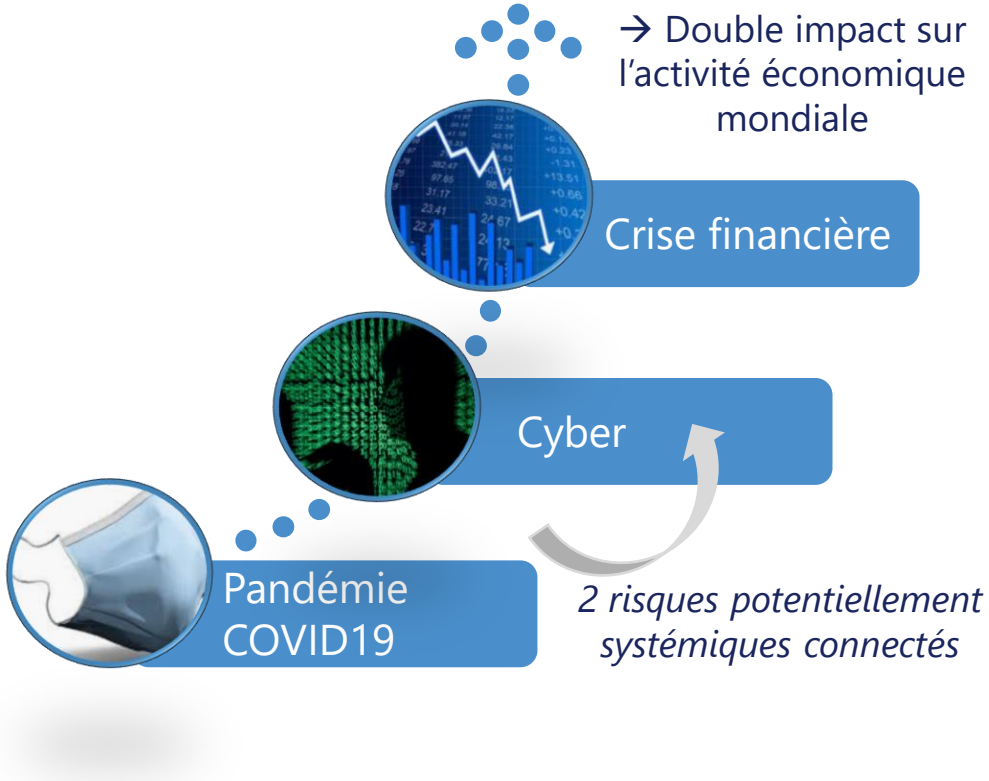
Protection des actifs dit immatériels ou intangibles ne trouvent aujourd'hui **aucune réponse assurantielle satisfaisante**.

addactis
THE RISKTECH FOR INSURANCE

Les enjeux réglementaires et assurantiels face au risque Cyber

Spéciale actualité COVID 19

Le Cyber : L'autre risque épidémique du COVID 19



Une mise en œuvre non-maîtrisée du télétravail

Que couvrent les polices Cyber ?

- Pas d'exclusions spécifiques à la notion de pandémie.
- Pas d'exclusions de l'utilisation des appareils personnels pour autant que les mesures de sécurité soient effectives
- Pas de couverture en cas de défaillance informatique généralisée liée à une panne internet ou réseau électrique (Risque systémique)

Un débat pourrait s'ouvrir sur la notion de modification voire d'aggravation du risque.

COVID 19 : Cas de force majeure ?

La qualification reviendrait alors au juge et serait très certainement au cas par cas.

addactis
THE RISKTECH FOR INSURANCE

Les enjeux réglementaires et assurantiels face au risque Cyber

Le Règlement Général sur la Protection des Données (RGPD) du 25 mai 2018

Sensibilisation des grandes entreprises aux risques de pertes de données

La sanction est dissuasive :

jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial.

Communiqué de l'ACPR le 12 novembre 2019 sur la distribution des garanties contre les risques cyber.

Clarification de sa position :

une de ses priorités de contrôle

addactis
THE RISKTECH FOR INSURANCE

Les enjeux réglementaires et assurantiels face au risque Cyber

❑ Identification des axes d'amélioration par l'ACPR

1. **Mesurer les expositions** affirmatives et silencieuses en **Cyber** présentes dans les polices DAB et RC et **les intégrer dans l'ORSA**
2. Besoin de **bases statistiques fiables**, alimentées par des données homogènes et répertoriées selon une **nomenclature stable et partagée**.
3. Les **offres** d'assurance doivent être clarifiées et **sans ambiguïté**
4. **La Cyber résilience doit devenir un axe majeur**

addactis
THE RISKTECH FOR INSURANCE

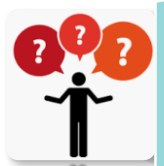
Les enjeux réglementaires et assurantiels face au risque Cyber

Assurance des risques cyber : un marché en phase d'expérimentation

L'hétérogénéité des propositions sur un risque jeune

Des assureurs extrêmement prudents.

Un risque difficile à appréhender, évolutif et très coûteux.



Face à l'absence d'historique sinistre, une prime souvent totalement inadaptée.

> **« Une cyber-réassurance encore à inventer »**

> **« L'argument financier immédiat pèse lourd dans la balance »**

Une **police cyber** : **création d'une ligne budgétaire nouvelle** pour les entreprises.

Une **approche graduelle** souvent adoptée chez les grands comptes

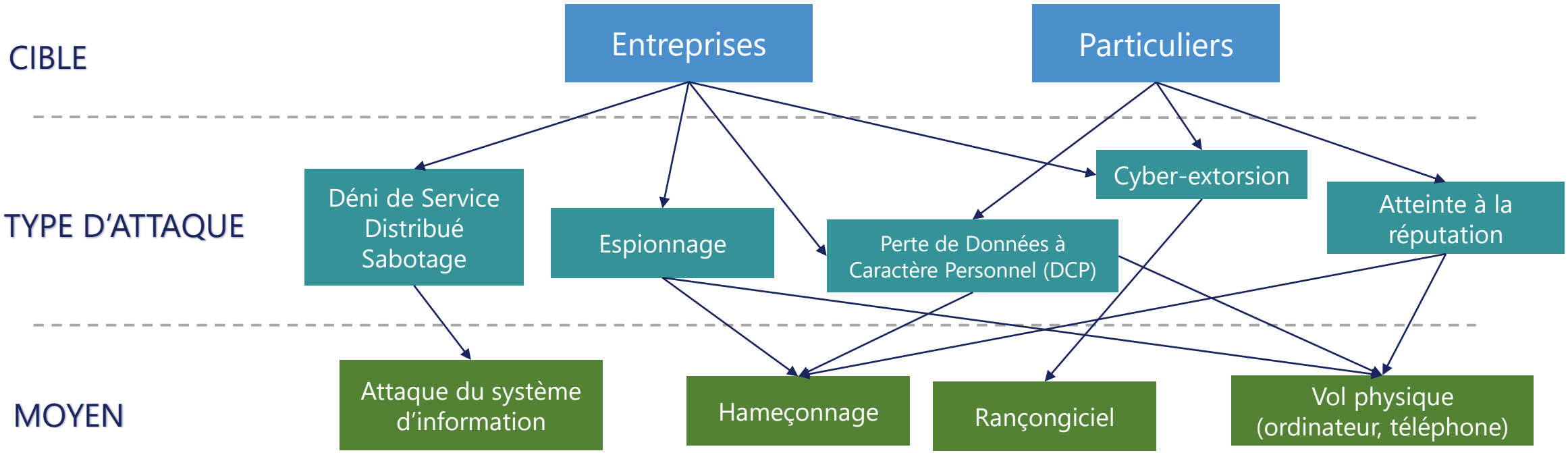
addactis
THE RISKTECH FOR INSURANCE

03 – Le challenge des actuaires

Aperçu des types d'attaques Cyber

La perte de DCP est l'unique risque de masse auquel sont exposés les particuliers

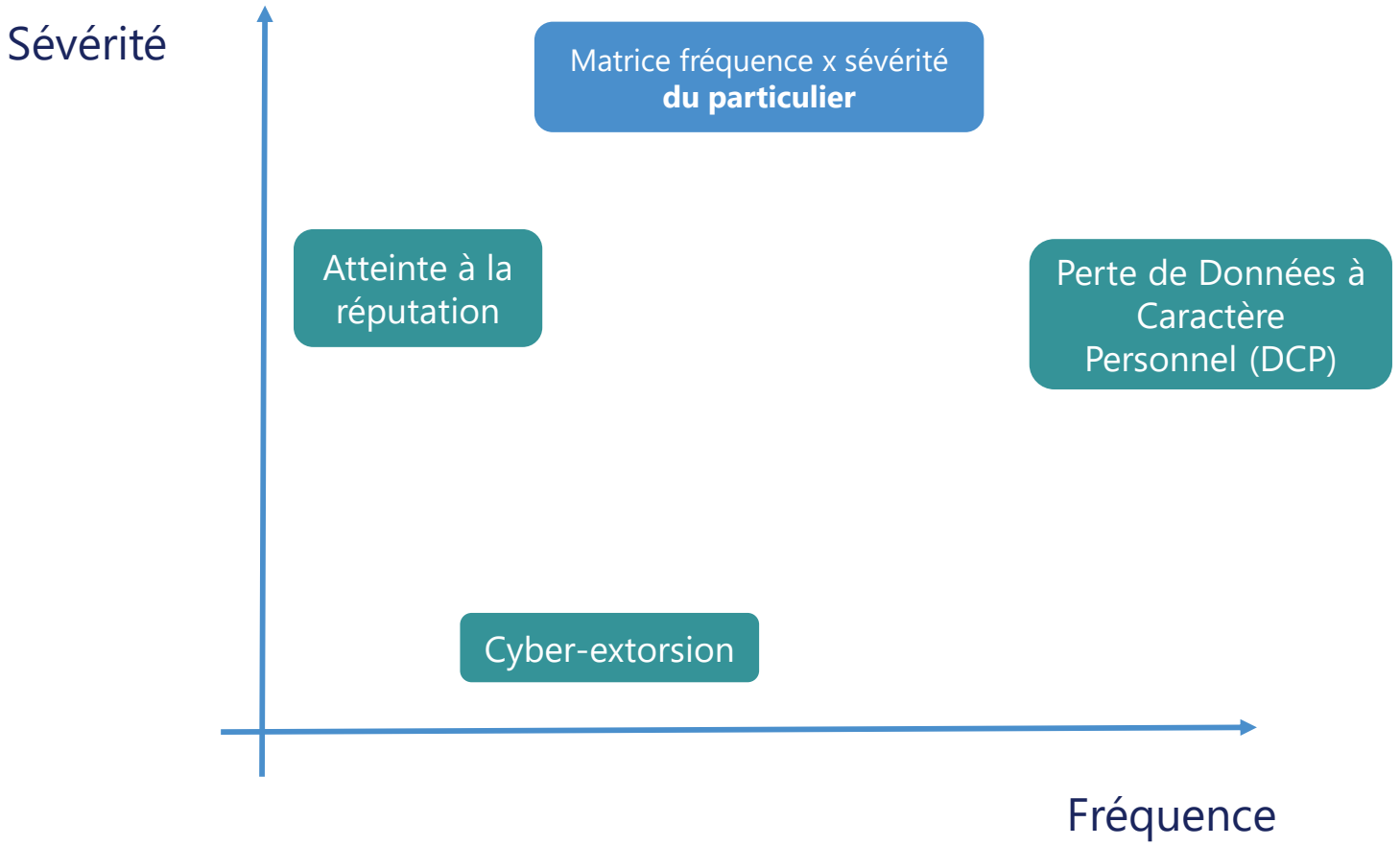
"Les particuliers sont exposés soit en direct (extorsion et atteinte à la réputation) soit via des entreprises (pertes de DCP)."



addactis
THE RISKTECH FOR INSURANCE

Exposition du particulier aux attaques Cyber

La perte de DCP est probable chaque année pour un particulier



Les pertes de DCP liées à des défaillances d'entreprises sont fréquentes et concernent à chaque fois un grand nombre d'individus.

La sévérité de la perte de DCP est très variable et peut être quasi nulle à très élevée (ex: usurpation d'identité, informations médicales).

addactis
THE RISKTECH FOR INSURANCE

Modélisation de la perte de DCP par des entreprises

Modélisation séquentielle de la sévérité, avec deux modèles

Variables en entrée

- Taille de l'entreprise
- Nombre de DCP dans le SI

Modèle de nombre de DCP perdues

Variables en entrée

- Zone géographique et réglementaire
- Secteur d'activité
- Niveau de maturité en Cyber-sécurité

Modèle de coût (€ / $)

*" Cette modélisation prend en compte les **spécificités de chaque entreprise** "*

Deux bases de données ont été étudiées : la base PRC (Privacy Rights ClearingHouse) et la base VERIS (Veris Community Data Base). Chaque base contient environ 8 000 sinistres, impliquant majoritairement des entreprises aux Etats-Unis.

La base VERIS satisfait mieux aux critères de Qualité Des Données définis par Solvabilité 2 et permet de calibrer le modèle de coût. La base PRC ne contient pas de variable de coût.

Modélisation du logarithme du nombre de DCP perdues

"La variable étant trop dispersée, c'est son logarithme qui est modélisé."

La meilleure approche est un ajustement de distribution

Distributions testées

Gamma	Gamma tronquée
Log-normale	Log-normale tronquée
Normale	Normale tronquée
Weibull	Weibull tronquée

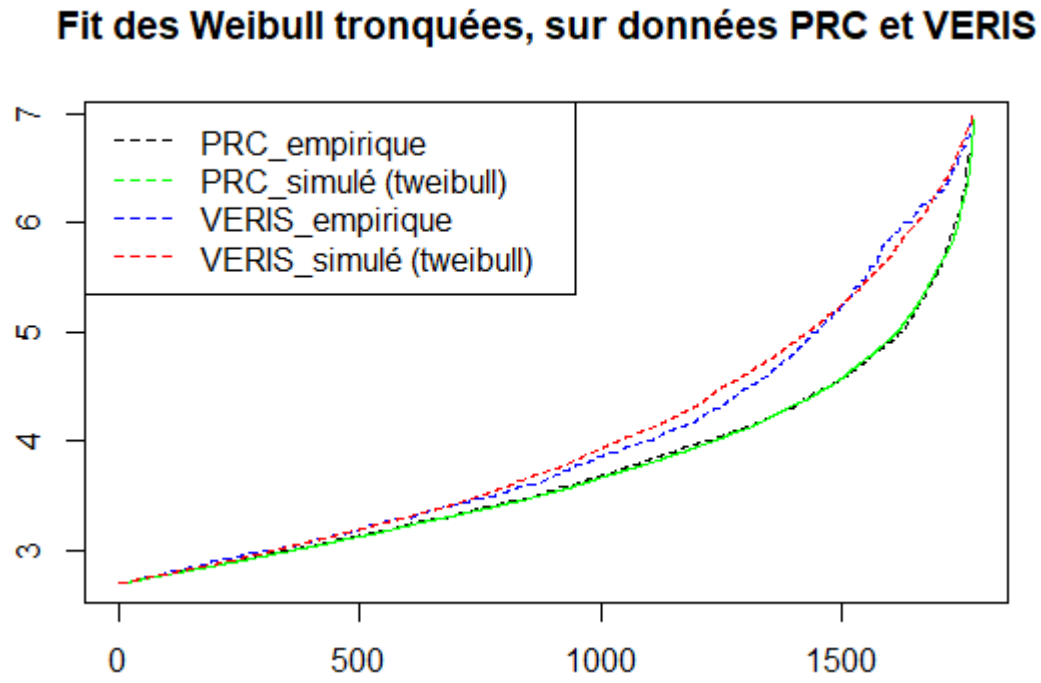
Distribution retenue

Weibull tronquée

Intervalle de validité qui dépend de la taille de l'entreprise

500 à 10 millions de DCP

La borne supérieure (10m) est réduite en fonction du nombre de DCP détenue par l'entreprise



Les lois de Weibull tronquée et Normale tronquée permettent chacune une modélisation satisfaisante, la loi de Weibull étant légèrement meilleure.

Ce n'est pas la forme de la distribution mais la base de données sous-jacente et sa représentativité du phénomène modélisé qui influe le plus sur la modélisation.

addactis
THE RISKTECH FOR INSURANCE

Modélisation du coût – 1/2

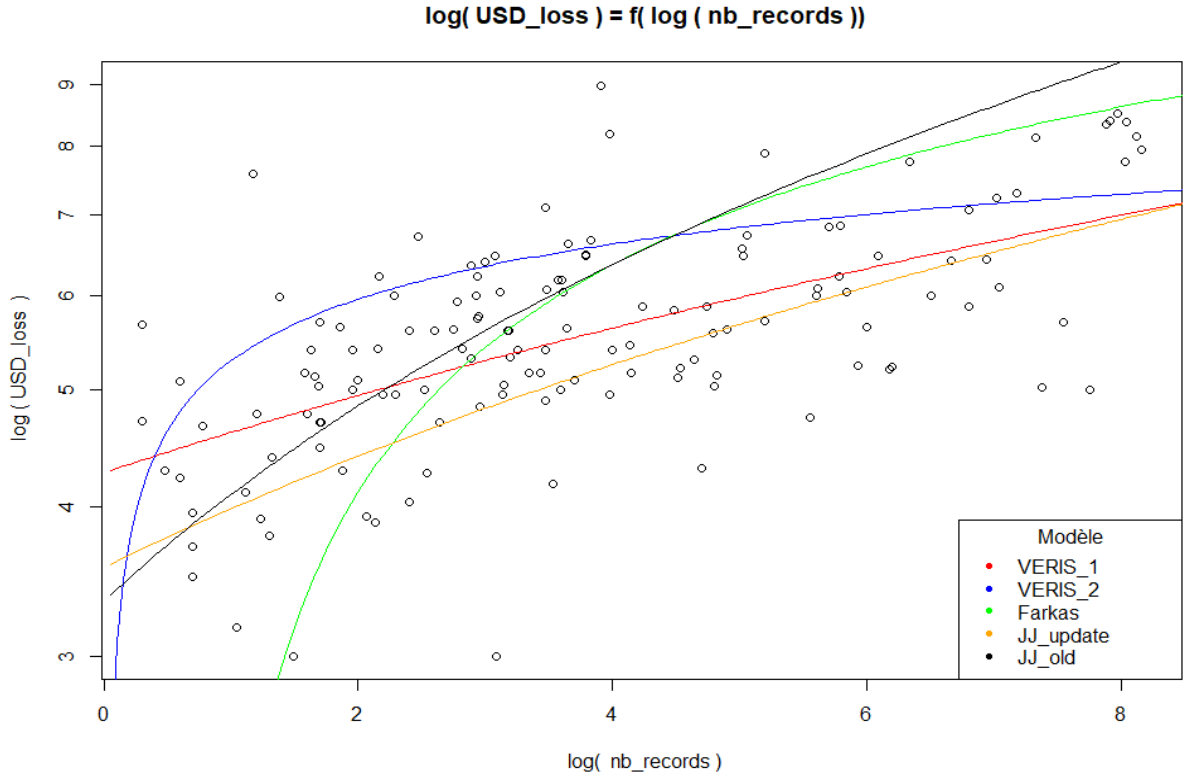
Deux modèles existants ont été étudiés et recalibrés

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

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

*Seul le **modèle Jacobs est adapté** aux petites et aux grandes pertes de DCP.*

*Recalibrer avec la **base VERIS** est pertinent car celle-ci contient **plus de données** et sont **plus récentes** que la calibration de Jacobs de 2015.*



VERIS_1 : modèle de Jay Jacobs calibré avec la base VERIS

VERIS_2 : modèle de Farkas calibré avec la base VERIS

JJ_update et JJ-old : Jay Jacobs a calibré son modèle en 2014 (JJ_old) puis en 2015 (JJ_update)

Modélisation du coût – 2/2

Ajustements spécifiques à l'entreprise

> *Les études conjointes de la base d'apprentissage et des caractéristiques du marché permettent d'* ***ajuster la modélisation aux spécificités de chaque entreprise***

Caractéristiques des entreprises de la base VERIS

- Secteur (sur représentation du secteur médical)
- Zone géographique (USA)
- Niveau de risque (moyen)

Caractéristiques de l'entreprise spécifique

- Secteur (ex : Finance / Assurance)
- Zone géographique (ex : France)
- Niveau de risque *(Faible / Moyen ou Elevé)*

Etude externe :

Ponemon et IBM (2019). Global cost of a data breach report.

Cette étude compare le coût des pertes en fonction des caractéristiques des entreprises.

addactis
THE RISKTECH FOR INSURANCE

Le savoir-faire d'Addactis

La modélisation

Construction des bases statistiques permettant de mieux délimiter les garanties Cyber et de les tarifer de façon pertinente.

Tarification : modèle de tarification Addactis du risque de perte de données et violation de confidentialité sur base d'une modélisation nombre de données perdues x Coût

Réassurance: à partir d'un modèle permettant une modélisation *From Ground Up* du risque Cyber, approche simulatoire coût – fréquence.

Focus sur les méga pertes de données (> 1m individus): Estimation du coût par donnée compromise.

Pour Répondre aux enjeux réglementaires

ACPR : Clarification des définitions et la terminologie relatives au risque Cyber pour que l'objet des garanties soit clairement défini

Pour le calcul du BGS, intégration du risque Cyber dans l'évaluation du Pilier 1 en modèle interne.

Réalisation d'un scénario ORSA calibré par ADDACTIS, selon les caractéristiques de l'entreprise : taille, exposition et niveau de Cyber-vulnérabilité

Approche Cat Man Made (Pilier 1) : sur base de jugement d'experts et de scénarios d'accumulation (évènements systémiques impactant une proportion conséquente du portefeuille d'assurés.)

04 ADDACTIS France vous accompagne

R&D Cyber 2020

Différents modèles pour différents périls Cyber

Les travaux présentés s'inscrivent dans une démarche globale de R&D au sein du cabinet.

Perte de Données à Caractère Personnel (DCP)

- Nombre de données perdues
- Modèle de coût

Déni de Service Distribué

- Durées d'interruption d'activité
- Taux de pénétration

Cyber-extorsion - Rançongiciel

- Modèle épidémiologique
- Modèle de diffusion

Les enjeux de recherche et développement sont relatifs à l'existence de données adaptées ainsi qu'à la culture du risque Cyber en France en en Europe.

La crise sanitaire actuelle nous a rappelé la fragilité et l'exposition de nos sociétés à certains risques.

L'actuaire a pleinement son rôle à jouer dans la quantification, la couverture et la sensibilisation de tous les acteurs de la société à ce type de risques dont le Cyber fait partie.

addactis
THE RISKTECH FOR INSURANCE

Merci de votre attention

contact-france@addactis.com

addactis
THE RISKTECH FOR INSURANCE

ADDACTIS France
46 bis Chemin du Vieux Moulin, 69160 TASSIN LA DEMI LUNE- Tél : +33 (0)4 72 18 58 58.
SAS au capital de 100 000 Euros
Immatriculée au RCS de Lyon sous le numéro 413 611 344
Numéro de TVA Intracommunautaire : FR 53 413611344
Organisme de formation agréé sous le numéro : 82 69 06035 69

ACTUARIAL COLLOQUIUM PARIS 2020

Disclaimer:

The views or opinions expressed in this presentation are those of the authors and do not necessarily reflect official policies or positions of the Institut des Actuaires (IA), the International Actuarial Association (IAA) and its Sections.

While every effort has been made to ensure the accuracy and completeness of the material, the IA, IAA and authors give no warranty in that regard and reject any responsibility or liability for any loss or damage incurred through the use of, or reliance upon, the information contained therein. Reproduction and translations are permitted with mention of the source.

Permission is granted to make brief excerpts of the presentation for a published review. Permission is also granted to make limited numbers of copies of items in this presentation for personal, internal, classroom or other instructional use, on condition that the foregoing copyright notice is used so as to give reasonable notice of the author, the IA and the IAA's copyrights. This consent for free limited copying without prior consent of the author, IA or the IAA does not extend to making copies for general distribution, for advertising or promotional purposes, for inclusion in new collective works or for resale.