Construction d’une base de données d’incidents cyber virtuels pour la calibration de méthodes actuarielles

Justin KHER

Hugo RAPIOR

Maud THOMAS

Sommaire

1 – Le risque cyber : les problèmes posés par le manque de données

2 – Construction d'une base de données

a) Un modèle hiérarchique pour relier les différents facteurs de risque

b) Catégories de cyber incidents

c) Prise en compte des conséquences d'une cyber attaque

3 – Zoom sur l'interruption d'activité

a) Le cas de l'attaque par déni de service

b) Interruption longue d'activité

4 - La prévention : procédure de prévention et de gestion de l'incident

5- Utilisation et perspectives

Risques émergents

- **Risques émergents** : un risque nouveau, ou connaissant une évolution nouvelle.
- Exemples :
  - risque épidémiologique (ancien mais avec survenance brutale d'un contexte nouveau)
  - risque climatique (évolution diffuse)
  - **risque cyber** (nouveau dans sa nature)
- Problème d'assurabilité :
  - l'évolution nécessite l'ajustement des modèles
  - on souhaite assurer de nouveaux risques (publics nouveaux, ou périmètre nouveau)

Quelques éléments de contexte dans le domaine du cyber

- Enquête AMRAE 2022 (sur sinistres 2021) :
  - enquête réalisée sur l'ensemble des courtiers opérant sur le marché français
  - pointe une baisse (4,4%) de couverture sur les grandes entreprises
  - la baisse est interprétée comme liée à un durcissement des conditions de couvertures (limites de polices en baisse, franchises en hausse)
- (Note : l'enquête 2023 présente un tableau bien plus favorable, mais fragile sur les PME, qui affichent des S/P importants)
- Postulat : une partie de ces conditions défavorables est liée à une mauvaise connaissance du risque.
- Données rares pour évaluer le risque, ou fragmentées entre différentes sources.

But de l’exposé

- Ce travail présente une méthodologie de création d’une base de données virtuelles qui permet de calibrer des modèles faisant la synthèse de différentes sources d’information « macros » disponibles sur le marché.
- Au-delà de la base elle-même, on discute de la possibilité de simuler des portefeuilles au-delà du public actuellement couvert par l’assurance.
- Volonté de fournir un cadre :
  - transparent
  - facile à mettre à jour
  - généralisable à d’autres risques

Construction d’une base de données d’incidents cyber virtuels pour la calibration de méthodes actuarielles

Le risque cyber: quantification, scenario de stress, mitigation et assurance

Olivier Lopez

Michel Denuit

Julien Trufin

Mario Ghossoub

Maud Thomas

Hugo Rapior

Justin Kher

Cyber Risk : Quantification, Stress Scenarios, Mitigation, and Insurance

Olivier Lopez[1,2], Michel Denuit[3,4], Mario Ghossoub[5], Julien Trufin[3,6], Justin Kher[1], Elisabeth Raes[3], Hugo Rapior[1], Mohammed-Amine Skoubani[1], Brieuc Spoorenberg[3]

November 19, 2023

Abstract

We discuss in this report the different challenges that appear in the quantification of cyber risk in the context of cyber insurance, and propose a methodology to develop a synthetic database of cyber events that may serve as benchmarks for risk analysis. This database is designed with the perspective of anticipating and optimizing risk transfer and risk management procedures. It can also be used to test the impact of different prevention schemes. Finally, we discuss the question of stress-testing insurance portfolios by analyzing how to calibrate different stress scenarios that may lead to a failure of mutualization. All the methodologies that are developed herein are presented in such a way that they could be quickly adapted and updated in light of new information and expertise, in order to take into account the evolution of the risk.

Key words: Cyber Risk, Cyber Insurance, Generalized Linear Mixed Models, Mixed Poisson Models, Cyber Risk Stress Scenarios.

Le risque cyber

Le risque cyber

Les problèmes posés par le manque de données

- Pallier le manque de données publiques
- Risque émergent en évolution rapide avec peu d’expertise
- Toute base est potentiellement biaisée
- Toute donnée historisée peut rapidement devenir obsolète
- Pas évident d’extrapoler la sévérité

  ➔Nécessité d’expert judgement

Objectif :

- Fournir une méthodologie à la communauté pour la construction d’un jeu de pseudo-données pouvant être simplement mis à jour

  ➔Pour benchmark les modèles actuariels

- Comprendre la nature du risque et toutes ses composantes pour définir des scénarios de stress

Le risque cyber

Les problèmes posés par le manque de donnéess

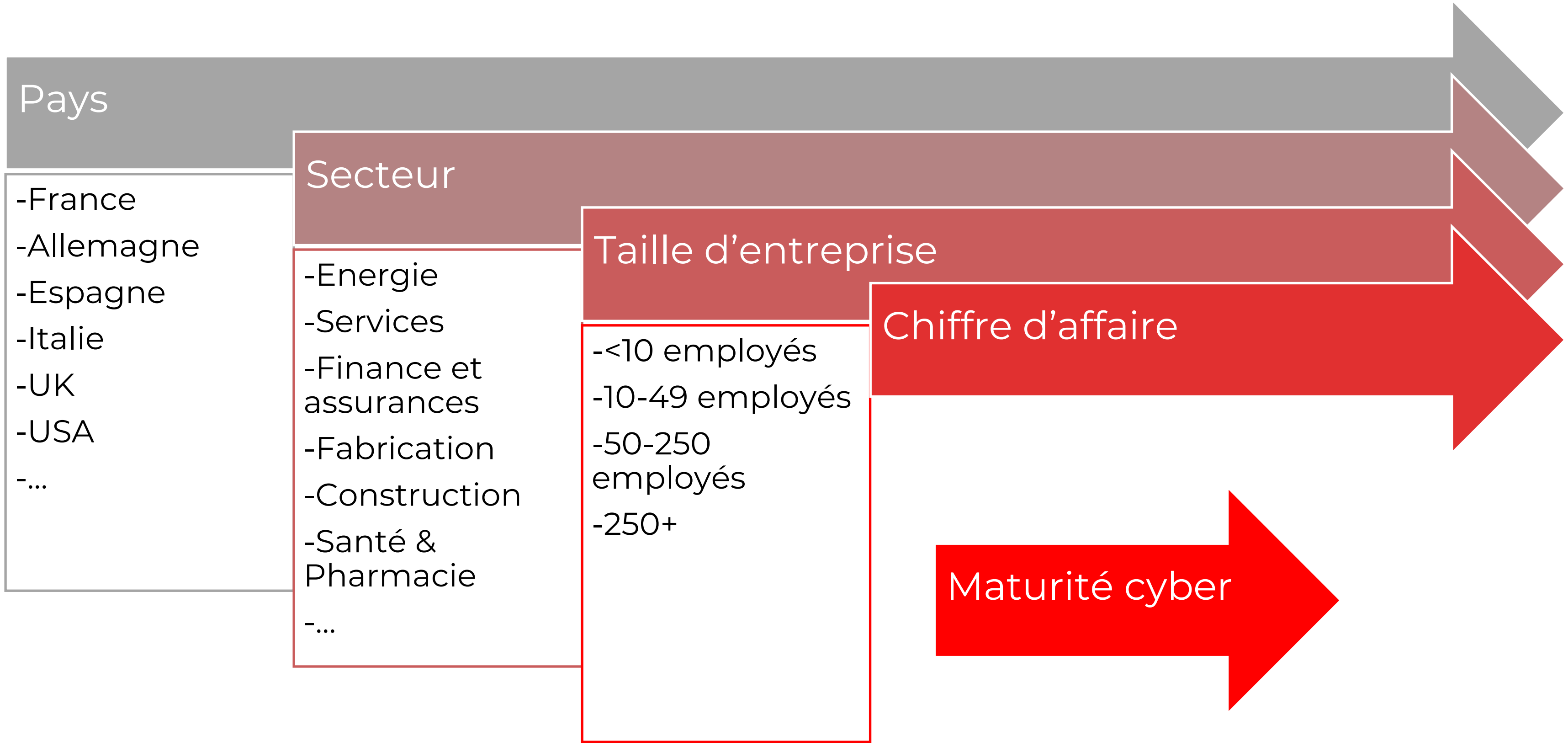
- Le risque cyber comprend une variété de situation
- Notre démarche s'appuie sur des sources variées

Documentation sur les incidents cyber et fuites de données personnelles	Suivi du risque	Attaque du cloud et Business interruption	Zoom sur le DDOS
• PRC database • VERIS database	• Rapport annuel IBM, *security data breach* • Rapport annuel Hiscox	• Lloyd's , *Cloud Down Impacts on the US economy* • Rapport annuel *IBM, security data breach* • Rapport *Flexera, State of the Cloud report*	• Rapport NSFocus,2022 Ddos

Construction de la base de données

Construction de la base de données

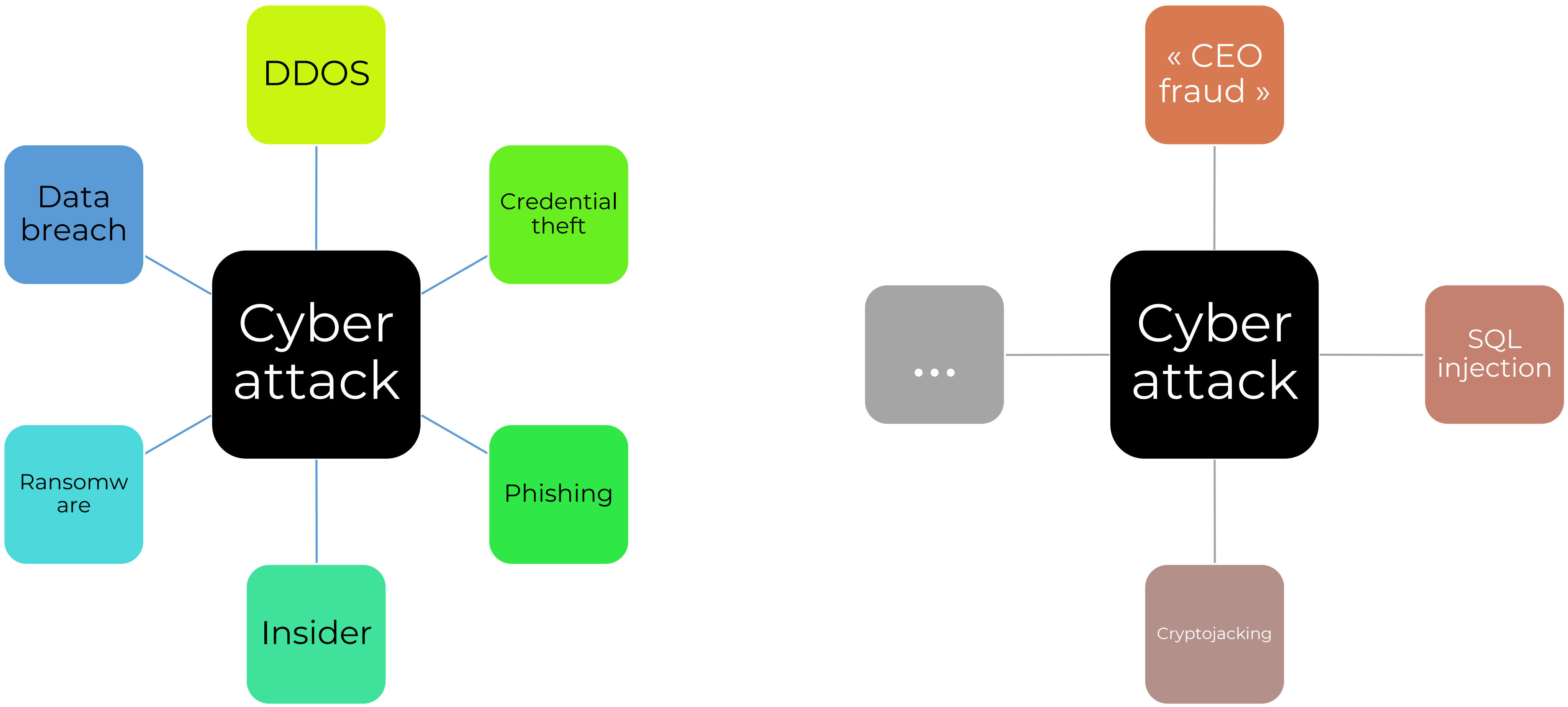
a) Un modèle hiérarchique pour relier les différents facteurs de risque



- Toutes ces variables ont potentiellement un impact sur la sinistralité cyber
- Données OCDE -> permet de générer un portefeuille fictif d'assurés représentatif de l'économie
- Paramétrisation pour générer la structure d'un portefeuille

Construction de la base de données

b) Catégories de cyber incidents



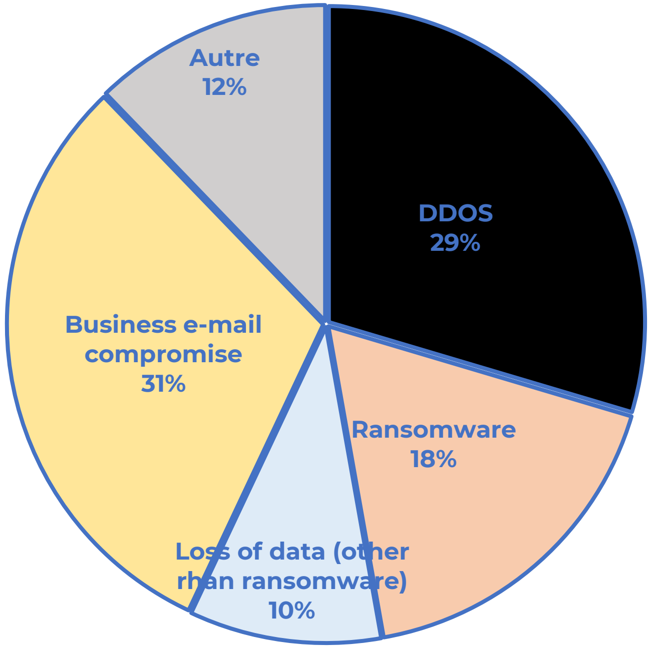
Construction de la base de données

b) Catégories de cyber incidents

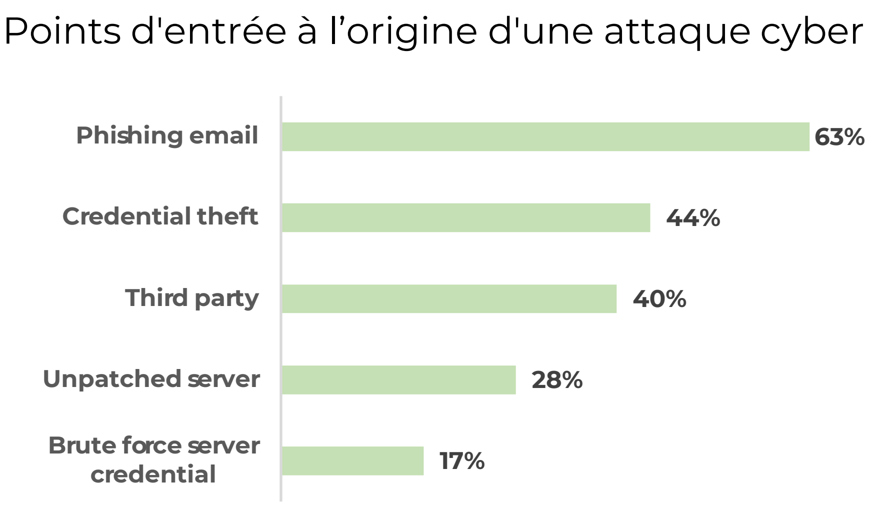
Interruption d'activité **courte** mais couteuse

Interruption d'activité plus **longue** (rançongiciel, indisponibilité du Cloud…)

Type of attack q	Entry point v
Ddos	Phishing email
Ransomware	Credential theft
Loss of data (other than ransomware)	Third party
Business e-mail compromise	Unpatched server
Other	Brute force server credential



Distribution du type d'attaque



Distribution des points d'entrée

Construction de la base de données

c) Conséquence financière d’une cyber attaque

Approche

- Modéliser les conséquences physique d’une attaque puis son véritable coût
- La sinistralité simulée est une combinaison de données historiques et de jugement d’expert
- Les coûts et leur repartition doivent dépendre des caractériques de la victime

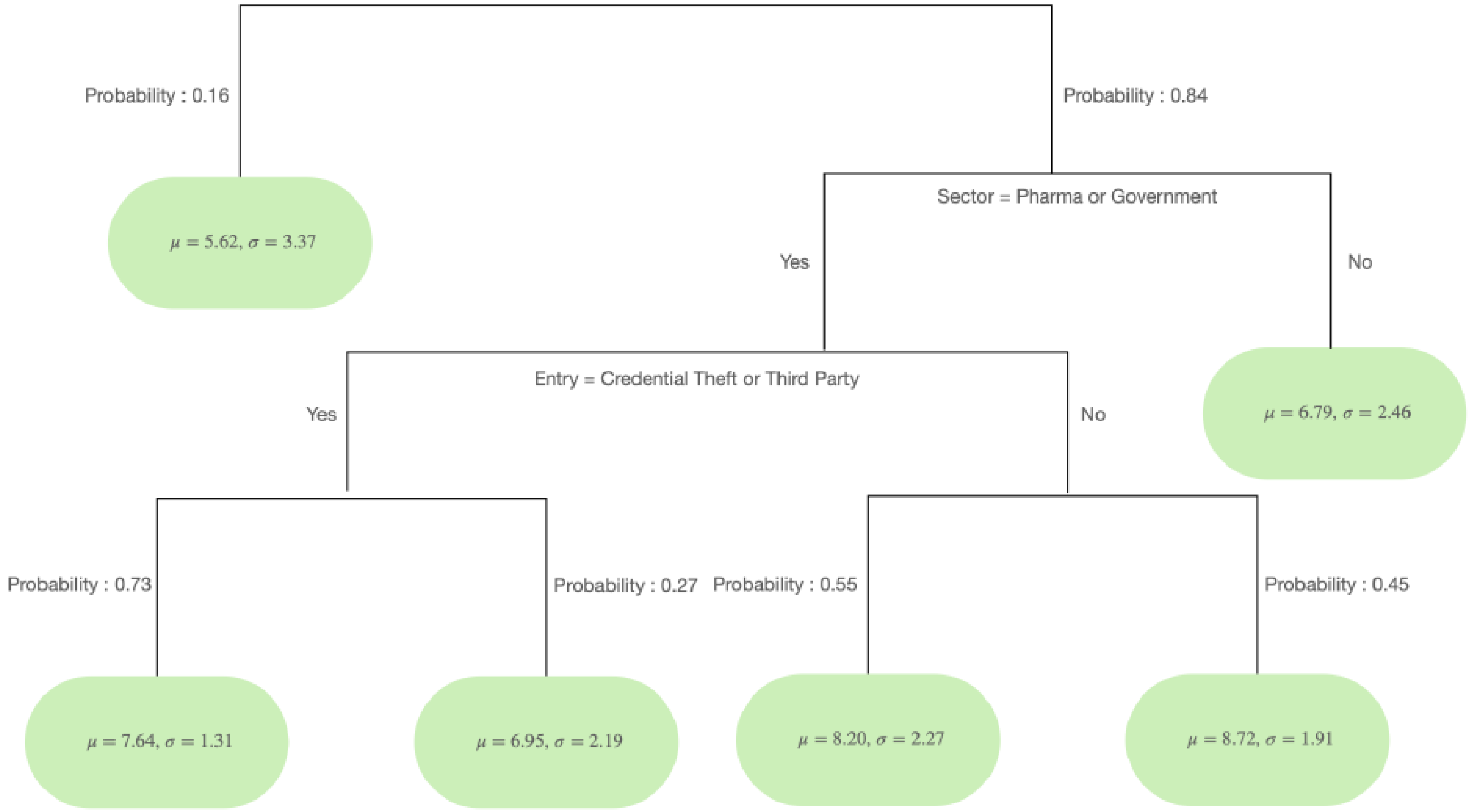
Plusieurs composantes

- La capacité d’une entreprise à se défendre et minimiser sa perte financière
- Le volume de données exposées en cas de vol ou de compromission des données
- La durée de l'interruption de l'activité

Volume de données compromises

Volume de données compromises

a) Sinistres attritionnels

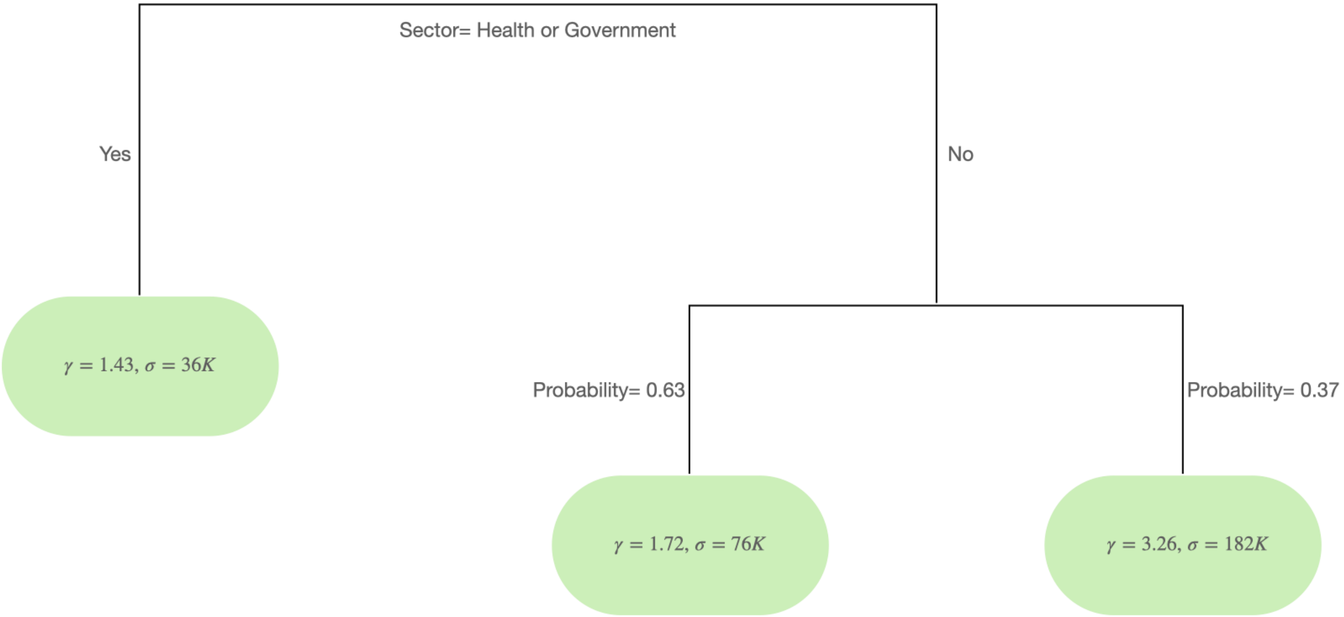


- « number of records » volume de donnée perdu
- Informations statistiques provenant de plusieurs sources (PRC, Veris...)

- Le point d’entrée a un impact sur le volume de donné leaké

Adaptation of Farkas, Lopez, Thomas (2021)

Volume de données compromises
b) Sinistres extrêmes



Adaptation of Farkas, Lopez, Thomas (2021)

Seuil u = 27 999

Loi de Pareto généralisée de paramètres (σ, γ) avec $\gamma>0$ et $R > u$

$$\mathbb{P}(R - u \geq t) = \frac{1}{\left(1+\frac{\gamma t}{\sigma}\right)^{1/\gamma}}$$

- La taille de la brèche n’est pas le seul marqueur de sévérité (exemple : DDOS)
- Business Interruption

Zoom sur l’interruption d’activité

Zoom sur l'interruption d'activité

a) Le cas de l'attaque par déni de service

- Interruption courte, généralement moins d'une journée
- Les attaques Ddos n'impliquent pas nécessairement de données compromises mais des coûts d'interruption élevés et variables
  - *Ponemon institute (2012) estime le c*oût moyen à 22K$ /minute
  - Le rapport *NSFocus* (2022) estime le coût entre 1 et +100K$/minute

Durée	< 5 min	5-10 min	10-60 min	1-12h	>12h
Proba	25%	36%	30%	7%	2%

NSFocus,2022

Durée d'une attaque DDOS

- En raison de la rareté de ces événements, des hypothèses doivent être envisagées pour traiter ce cas particulier
- Peu de statistiques disponible sur les attaques Ddos > 12h

Zoom sur l’interruption d’activité

b) Interruption longue d’activité (rançongiciel, indisponibilité du Cloud…)

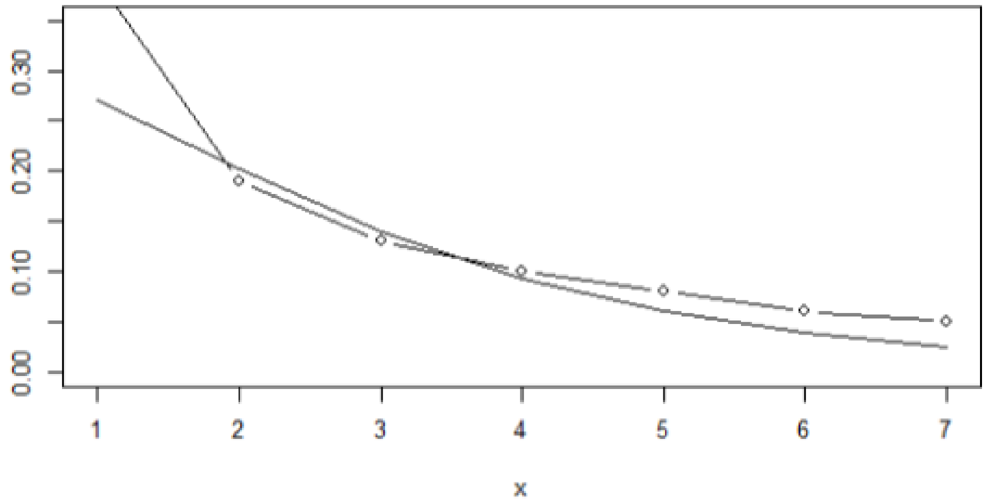
Première interruption → Plan de secours qui réduit les dommages causés → Restauration du système d’information → Retour à la normale

Estimation de l’interruption d’activité à partir des interruptions du cloud

Durée	1	2	3	4	5	6	7
%	39%	19%	13%	10%	8%	6%	5%

Temps nécessaire (en jour) pour atteindre zéro perte une fois que le service vers le cloud rétabli

Loi Gamma →



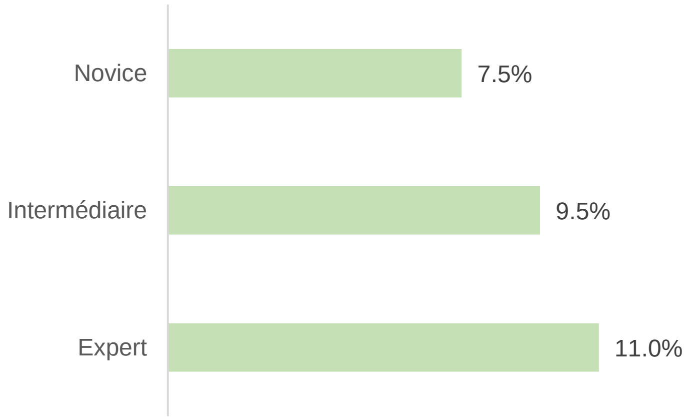
Lloyd’s Cloud Down Impacts on the US economy

Calibration d’une loi gamma pour capter des interruption plus longues

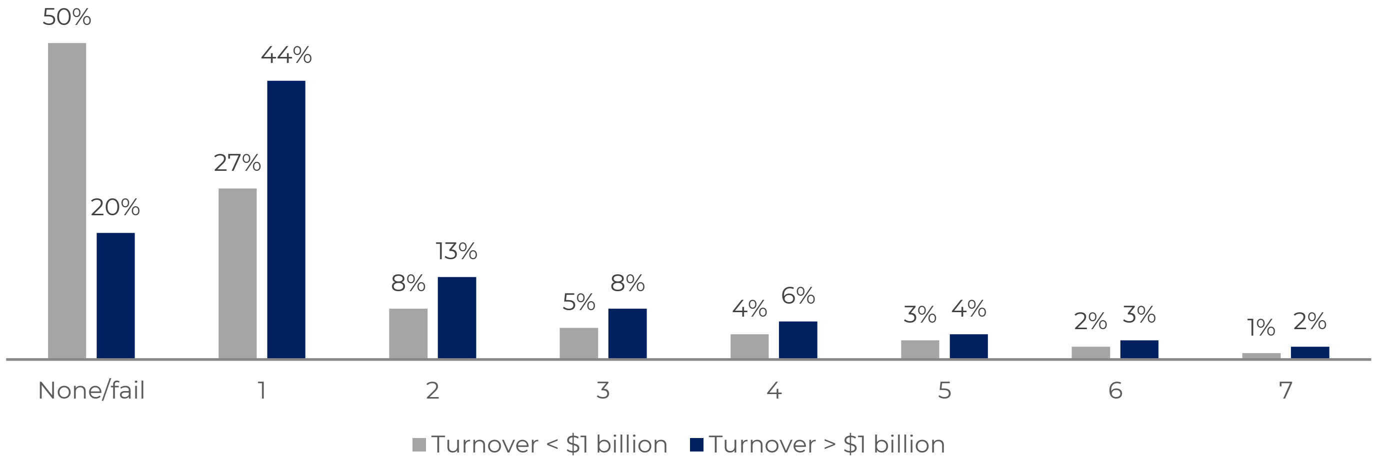
Zoom sur l'interruption d'activité

b) Interruption longue d'activité (rançongiciel, indisponibilité du Cloud…)
Réduction des dommages

Probabilité de défense contre une attaque



Probabilité d'implémenter un plan back-up selon le CA d'une compagnie



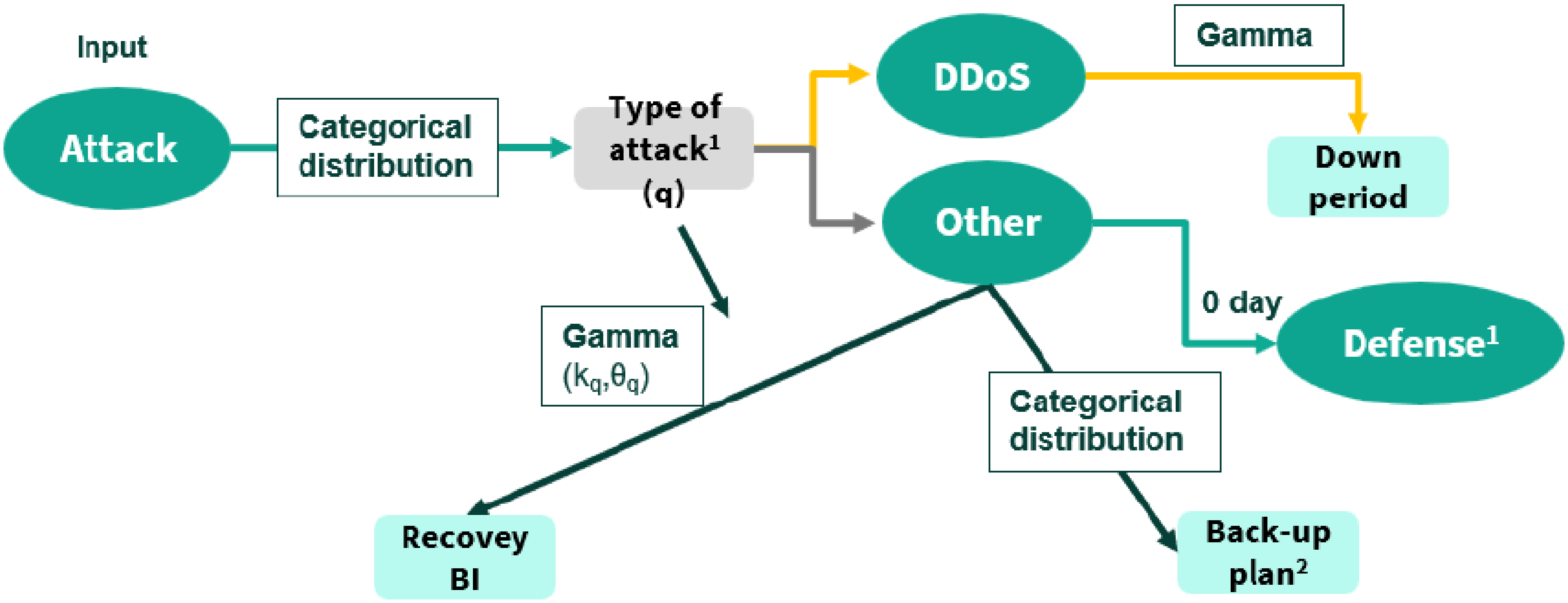
Lloyd's Cloud Down Impacts on the US economy

Interruption initiale	Début d'un plan de récupération	Temps de retour à la normale	Perte
1 jour	Aucun	Jour 3	4,5M$
3 jours	Jour 2	Jour 5	4,7M$
5 jours	Jour 3	Jour 7	6,8M$

Exemple pour une entreprise de 500M$ de CA

Zoom sur l'interruption d'activité

c) Schéma récapitulatif



La prévention

La prévention

Comment valoriser la prévention ?

Exemples :

- Protection Ddos

- Prevention du phishing

- Efforts dans la gestion de crise générée par une attaque

- Zoom sur la réalité du marché

Lien avec un cadre bayésien

Cadre bayésien

Illustration

- Considérons le nombre de sinistres subis par un assuré d’une certaine catégorie.
- On dispose d’un historique (généralement faible) sur cette catégorie d’assurés, échantillon $N_1, \dots, N_n$
- L’approche bayésienne consiste à introduire un facteur de risque θ caché, dont on connaît la distribution.
- Formellement,
  - $N_1, \dots, N_n \mid \theta$ suit une certaine loi P_θ
  - θ est le résultat d’un tirage aléatoire (dont le résultat n’est pas visible) selon une loi *a priori* π.

Cadre bayésien

Illustration

- Exemple : $N_1, \dots, N_n \mid \theta$ suivent une loi de Poisson de paramètre θ
  - θ représente la fréquence de sinistres, qui va être différent suivant que la population est très exposée au risque ou non.
  - La loi *a priori* représente alors la répartition des θ dans la population générale.
- L'estimation bayésienne consiste à estimer θ en combinant données historiques et en utilisant l'information contenue dans cette loi *a priori*.

- **Question cruciale** : comment choisir cette loi a priori ?

Cadre bayésien

Illustration

- Les travaux menés ici peuvent servir à construire une loi *a priori*.
- Ils reflètent une vision globale du risque.
- Le portefeuille d'assurance n'est pas représentatif de la population globale, mais l'historique dont on dispose va permettre de s'éloigner de cette distribution globale.
- Méthodologie non spécifique au cyber : travaux en cours (Antoine Heranval, Olivier Lopez, Maud Thomas) issus d'une collaboration avec la Mission Risques Naturels qui appliquent le même type de techniques (avec une base de données non simulée contrairement au cas présent)

Conclusion

- Manque d’expérience et de données historiques pour fournir une analyse du risque, le calibrer et l’évaluer
- Pour réduire le faussé causé par le manque de données, nous avons construit une base fictive d’événements
- L’objectif est de mieux comprendre la nature du risque et toutes ses composantes et de pouvoir être utile pour définir des scénarios de stress
- L’outil doit être flexible afin d’être conforme au point de vue de l’utilisateur final
- Les paramètres utilisés pour simuler cette base de données ont vocation à être mis à jour dans un processus de mise à jour périodique
- Ces techniques doivent être adaptées avec les évolutions sur le risque cyber, ou tout autre risque considéré