17e Congrès des ACTUAIRES

en partenariat avec

BANQUE DE FRANCE
EUROSYSTÈME

CRÉATION ET MANAGEMENT STRATÉGIQUE DE LA VALEUR :

LES NOUVEAUX LEVIERS

INSTITUT DES ACTUAIRES

15 juin 2018

Hôtel Marriott Rive gauche

INSTITUT DES ACTUAIRES

Évaluer le cyber-risque : un enjeu majeur pour la création de valeur

Atelier coordonné par Florence Picard
Intervenants : Mary-Cécile Duchon (ACPR), Caroline Hillairet (Ensae Paris-Tech), Olivier Lopez (ISUP Sorbonne Université), Alexandra Maunié-Foucart (AXA GRM)

Les points de vigilance de l'ACPR vis-à-vis du risque cyber

Dimension Cyber sécurité

- points contrôlés par l'ACPR dans le cadre de solvabilité 2
- Publication d'un discussion paper ACPR (fin : 15/06)
- Au niveau de l'IAIS, premier issue paper en 2016
- Au niveau FSB, discussion du cyber lexicon
- Questionnaire EIOPA intégrées au stress-test

Cyber attaques

Dimension Cyber assurance

- grande vigilance de la part des superviseurs
- Différentes enquêtes / revues en cours (ACPR, EIOPA, etc,)

Cyber assurance

Des attentes réalistes à destination du marché

#1 Gestion des risques de souscription plus effective :

revue des portefeuilles (couverture silencieuse)

évaluation appropriée et veille réglementaire

#2 Amélioration de la compréhension interne du risque cyber

incluant une meilleure collecte de données

#3 Garantir une communication claire sur les nouveaux produits

clarification des clauses contractuelles

clarification du rôle de chaque acteur (assureur / intermédiaire / réassureur)

Une supervision resserrée pour un développement raisonné et contrôlé

- Promotion d'un développement contrôlé dans le respect des cadres réglementaires
  - lutte anti-blanchiment, assurabilité, gouvernance adaptée
  - Analyse approfondie du risque cyber basée sur des données de qualité suffisante

- Surveillance, coordination & supervision adéquate favorisant un marché résilient et plus stable

- Réseau interdépendant : la probabilité d'attaque de chaque noeud du réseau dépend
  - **de son niveau de sécurité (attaque directe)**
  - **du niveau de sécurité des autres noeuds du réseau (attaque indirecte)**

- Modèle d'investissement en matière de sûreté (filtres anti-virus, pare-feu, système de détection d'intrusion)
  - **Les firmes sont risques averses**
  - **l'investissement en matière de sûreté génère une externalité positive**
  - **Il peut être plus attractif de compter sur la sécurité des autres noeuds que d'investir dans la sécurité de sa propre entité**

- Cyber-assurance
  - **besoin d'information sur les interconnections et le niveau de sécurité des nœuds interconnectés**
  - **Cyber-assurance (avec contrôle des termes du contrat) pourrait apporter des incitations vers un plus fort niveau d'investissement en matière de sécurité.**

- Modèles de contagion en épidémiologie (vaccination)

- Un équilibre (de Nash) est un niveau de protection de chaque nœud pour lequel il n'est pas optimal pour aucun nœud de modifier son niveau de protection

- Caractérisation du niveau de protection à l'équilibre
  - **Il n'est pas toujours socialement efficace: l'individu a tendance à sous-investir par rapport à l'optimum social, notamment si il y a un mauvais niveau d'information des protagonistes du réseau**
  - **Besoin de concevoir des politiques générant des incitations à augmenter le niveau de protection**
  - **Utilité d'un modèle qui permet de quantifier et de comparer les impacts de différentes politiques.**

INSTITUT DES ACTUAIRES

- S'inspirer des modèles de contagion en épidémiologie…avec la différence importante que dans un monde cyber, le "virus" (le hacker) est un agent stratégique.

- Modéliser les incitations des hackers :
  - **bénéfices d'une attaque: pécuniaire, idéologique…**
  - **coûts de l'attaque: équipements, temps et/ou effort**
  - **coûts pénal en cas d'arrestation**

- Modéliser les incitations des défendeurs:
  - **Coûts d'investir dans la protection: monétaire, temps et/ou effort**
  - **Bénéfices: réduit la probabilité d'intrusion et la taille des pertes.**

- Stratégies changent au cours du temps: aspect dynamique et aléatoire

INSTITUT DES ACTUAIRES

La faible qualité des données

- Les modèles considérés doivent prendre en compte la complexité du phénomène, notamment :
  - **Accumulation**
  - **Contagion**
  - **Évolution des comportements**
  - **…**
- Ces modèles doivent être calibrés à partir des données.
- Les sources de données sont faibles, et leur qualité rare.
- Nécessité de comprendre la structure des données, et d'intégrer leur mauvaise qualité à la modélisation actuarielle mise en œuvre.

INSTITUT DES ACTUAIRES

Les sources de données publiques

- Différentes bases de données publiques informent sur le risque, par exemple :
  - **Bases de données sur les types de failles des logiciels**
  - **Bases de données américaines sur le nombre de « data breaches »**
- Les données sur les failles identifiées ne considèrent que des types d'incidents d'ores et déjà identifiés. Même si elles sont informatives, elles ne permettent pas totalement de projeter le risque.
- Les bases sur les « data breaches » sont entachées de biais.
- On pourra notamment trouver des références à ces bases dans le mémoire de Florian Pons (CNAM, 2014).

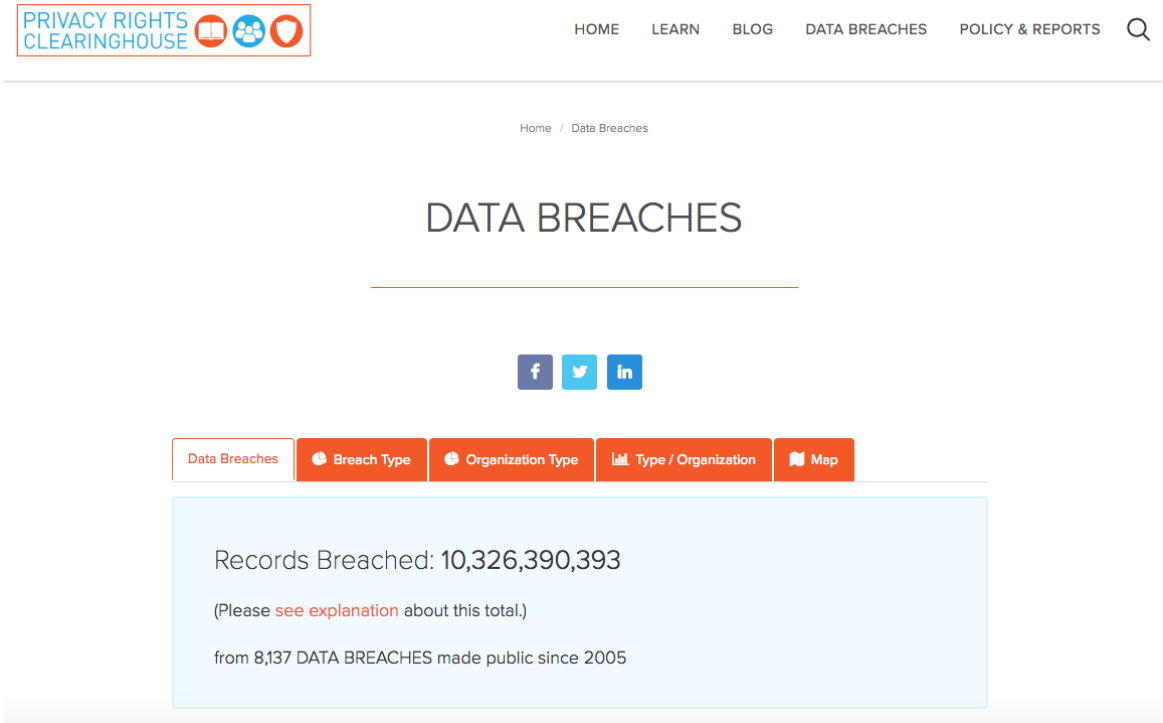
INSTITUT DES ACTUAIRES

Information manquante

- Les phénomènes à l'œuvre sont classiques, mais exacerbés par la nature du risque.
- On note notamment un biais de déclaration, proche du phénomène de « hunger for bonuses. »
- Hunger for bonuses : en assurance-auto, certains sinistres ne sont pas déclarés car conduiraient à un malus.
  - **Point positif : l'assureur paie moins « qu'il ne devrait »**
  - **Point négatif : l'assuré cache de l'information sur son risque**
- Ici, on peut notamment distinguer :
  - **Des petits incidents qui ne sont éventuellement pas vus par l'assuré**
  - **Des gros incidents qui sont tus**
  - **Ce comportement peut changer au cours du temps, notamment en fonction des obligations réglementaires (en terme de déclaration)**
- D'un point de vue statistique, il s'agit d'un **phénomène de troncature.**
- À ce phénomène s'ajoute, en assurance, aléa moral et antisélection.

L'exemple de la base « data breaches »

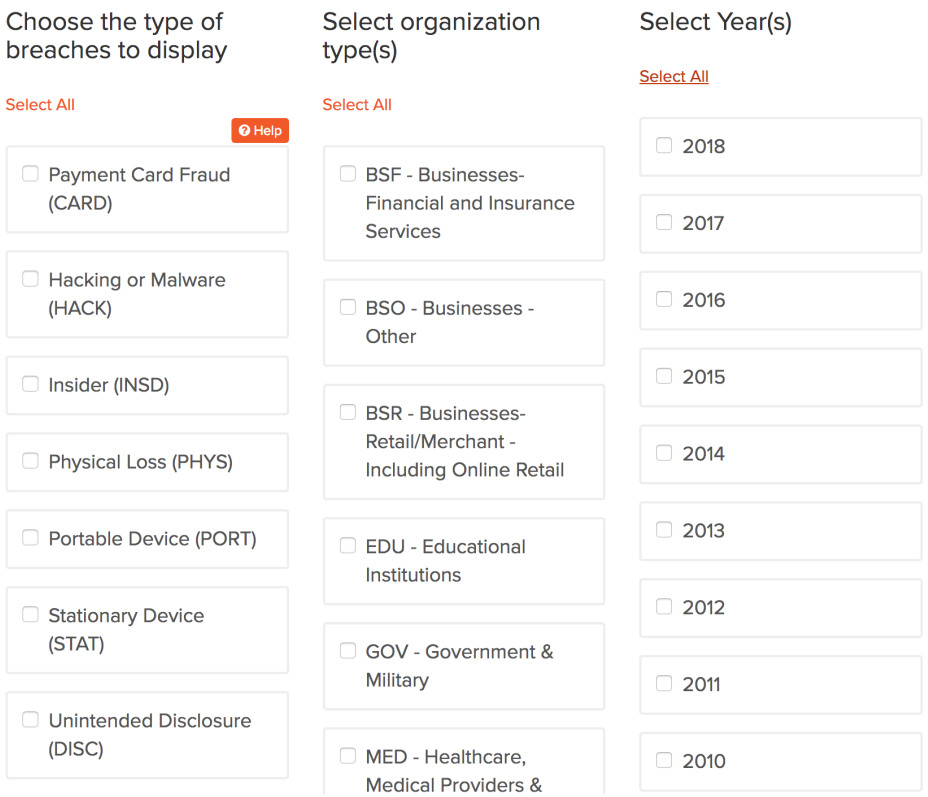
- La base est disponible à l'adresse :
  https://www.privacyrights.org/data-breaches



INSTITUT DES ACTUAIRES

L'exemple de la base « data breaches »

- Différents types de sinistres répertoriés par année et par secteur.



L'exemple de la base « data breaches »

- Outre l'instabilité du risque (changement de comportement des différents acteurs) la nomenclature des sinistres n'est pas nécessairement stable dans le temps :

Date Made Public	Type of breach	Type of organization	Total Records	Description of incident
December 14, 2008	HACK	BSR	0	Hackers broke into a Merrimack movie theater's servers and stole customers' credit card information.
September 30, 2008	HACK	EDU	11	A hacker attacked the University of Indianapolis' computer system and gained access to personal information and Social Security numbers for 11,000 students, faculty and staff,
September 19, 2008	HACK	EDU	31	A class roster was among some documents located on a computer server that was hacked. The class roster was for Economics-2301 held during the first summer session of 2004. Social Security numbers were part of the information on those documents.
August 14, 2008	HACK	MED	500	Hundreds of people in Brevard County found out their personal information was stolen. Names, Social Security numbers and even personal medical information were posted on the Internet.
August 12, 2008	HACK	BSF	5	Wells Fargo is notifying customers that hackers have accessed their confidential personal data by illegally using its access codes. Personal information including names, addresses, dates of birth, Social Security numbers, driver's licence numbers and in some cases, credit account information was accessed by unauthorised persons.
June 10, 2008	HACK	BSF	0	1st Source Bank is replacing ATM cards this month for all its account holders after cyber-thieves accessed an unknown amount of debit-related data.
June 4, 2008	HACK	EDU	4,7	The Oregon State Police are investigating the theft of personal information from online customers of the OSU Bookstore who used credit cards to purchase items.

Un risque est une opportunité. Pour qu'une opportunité se transforme en valeur, il faut pouvoir qualifier et quantifier le risque

INSTITUT DES ACTUAIRES

Du risque vers l'assurance

1. **Comprendre le risque**
2. **Définir une appétence au risque**
3. **Modéliser le risque**
4. **Piloter le risque**

1 – Comprendre le risque:

La nécessité d'un langage commun

- *Plusieurs travaux ont été menés pour qualifier ce que l'on peut appeler « l'évènement cyber », ses acteurs et ses conséquences:*
  - *Codification des garanties*
  - *Codification des sinistres*
- *Objectif: bâtir des bases de données marché d'évènements fiables*
- *Limites observées:*
  - *Non standardisation des garanties d'un marché à l'autre, d'un assureur à l'autre*
  - *Réticence à déclarer un sinistre (risque de réputation, risque d'image)*

La compréhension de la diffusion d'un évènement Cyber

- *Absence de frontières géographiques*
- *Facteurs de propagation: sensibilité de certains secteurs d'activité, vulnérabilité en cyber sécurité*

INSTITUT DES ACTUAIRES

2 – Définir une appétence au risque:

La perte maximale potentielle: *Combien s'autorise-t-on à perdre en cas de survenance d'un évènement majeur?*

La souscription du risque: *Quels clients, secteurs d'activité, zone géographique…?*

3 – Modéliser le risque

Les limites actuelles:

- *Absence de profondeur d'historique*
- *Fréquence: nombre limité d'évènements*
- *Environnement en mutation rapide: les évènements cyber d'aujourd'hui ne seront pas ceux de demain*

L' approche:

- *Définition de scénarios déterministes*
- *Collecte d'exposition: quelles garanties sont accordées à quel type d'assurés, opérant dans quel secteur d'activité, et pour quel montant d'indemnité?*
- *L' empreinte des scénarios est passée sur les portefeuilles d'exposition afin de déterminer le coût assurantiel d'un évènement majeur*

INSTITUT DES ACTUAIRES

4 – Piloter le risque:

- Mise en place d'une gouvernance « renforcée »
- Suivi régulier des expositions (= son développement commercial)
- Reporting sinistres
- S'autoriser à apprendre. Quand l'expérience passée n'est pas suffisante pour prédire la survenance future

Le risque cyber comme créateur de valeur:

- ***Dynamique d'un eco-système complet (Assuré, Fintech, Industrie (ré)assurance…)***
- ***L'assurance est un protecteur et vecteur de prise de conscience:***
  - ***pour l'entreprise:*** *vulnérabilité au risque et prévention*
  - ***pour le particulier:*** *protection de la vie privée*

INSTITUT DES ACTUAIRES

Questions ?

4, rue Chauveau-Lagarde - 75008 Paris - tél. 01 44 51 72 72 - fax 01 44 51 72 73
www.institutdesactuaires.com