www.institutdesactuaires.com

Éclairer les risques, tracer l'avenir

100% ACTUAIRES
8 NOVEMBRE 2016

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Introduction :

Présentation du Groupe de Travail Cyber Risk

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- Objectifs : Sensibiliser les actuaires à :
  - **L'importance du risque cyber**

  (Conférence du 7/06/16)
  - **L'émergence du marché de cyber assurance**
  - **Leur rôle dans la mesure et la gestion du risque**

- Travaux orientés sur 3 volets :
  - **Périmètre cyber : risques et assurance**
  - **Règlementation et normes, rôle de la prévention**
  - **Mesure des risques, rôle de l'actuaire**

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Participants au GT et sommaire de l'atelier

- 7 permanents
  - **Animation : Carole Mendy**
  - ***Enjeux du cyber risques; cartographie***

Philippe Talleux, Herbert Groscot

  - ***Règlementation, normes***

Yann-Hervé Beulze

  - ***Marché, mesures du risque***

Florian Pons, Antoine Brun

  - ***Rôle de l'actuaire***

Hélène Gelé

- Des participations ponctuelles (Thomas Chapuis)

Merci à Agnès Canarelli pour son soutien logistique

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

A signaler :

Autres travaux menés en parallèle

Travaux du groupe Big Data dont est issu le SGT Cyber Risk (un grand merci à Florence Picard)

Article a paraître en décembre 2016 :

Synthèse de nos réflexions et annexes documentaires réunis dans un article, comprenant notamment une analyse de la cartographie des contrats d'assurance face au risque cyber.

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

100% ActuaireS

INSTITUT DES ACTUAIRES

Enjeux du risque cyber

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **Définition**

Tout ce qui touche à l'atteinte, la violation ou la perte de données, ainsi qu'à des intrusions de réseau ou qui est relatif aux disfonctionnements d'un ensemble d'algorithmes, conduisant à des préjudices matériels, corporels ou portant sur des actifs immatériels et à la menace de telles situations.

- Les dommages associés aux cyber risques sont « en général » liés à des « délits » qui se manifestent par des « cyber attaques », des « intrusions », des exploitations de « failles de sécurité dans les systèmes d'information ».

- La nature des dommages consécutifs peut être matérielle, financière mais aussi corporelle.

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **Exemples (tous publics !)**

  - **Les cumuls :** « Dyn fournit des services de gestion de nom de domaine. Or celui-ci a déclaré avoir été la cible d'une attaque de déni de service […] Dyn est un fournisseur de DNS spécifique, [….] En faisant cela, les pirates ont réussi à perturber un plus large éventail de cibles parmi les organisations qui utilisent les services du fournisseur dont des sites de renoms tels que Box, CNN, Imgur, PayPal Twitter, Spotify, Github, Airbnb, Reddit, etc. » Source ZDNet- 21/10/2016.

  - **Données Bancaires :** En janvier 2016, le site "The Digital Reader" annonce un vol important de données clients à partir d'une base de données de Dell. De nombreux clients se sont fait appeler par des inconnus se faisant passer pour le support technique de Dell. Ces inconnus disposaient d'informations confidentielles (email, informations concernant les comptes clients). Ces appels se seraient produits durant plus de 6 mois avant la détection de la faille.

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **Exemples (tous publics !)**

  - **Données Médicales :** Le site pourquoidocteur.fr signale qu'en 2015 les établissements de santé ont été victimes de 1 300 cyberattaques. Ces attaques illustrent toutefois l'intérêt que portent les pirates informatiques à nos données de santé. Un dossier médical serait revendu 50 dollars (43 euros) contre une trentaine de dollars (26 euros) pour des codes de carte bancaire. Pour y accéder, les hackers utilisent de plus en plus des « rançongiciels ».

  - **Dommage Corporels :** En février 2016, l'hebdomadaire Le Point nous informe que les pacemakers sont dans le collimateur des pirates informatiques. Il serait possible de tuer des milliers de personnes d'un simple clic en s'en prenant aux pacemakers qui équipent 5 millions d'individus de par le monde. En France, actuellement un peu moins de 400 000 individus sont porteurs de stimulateurs cardiaques, Les pacemakers font parties des multiples objets connectés qui accompagnent de plus en plus notre quotidien.

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **Un risque assurable ? Un risque déjà assuré ?**
  - **Les dommages créé par le cyber risk sont polymorphes :**
    - **La (les) victime(s)**
      - La première catégorie regroupe des personnes physiques ou morales propriétaires des matériels et équipements ayant constitué les cibles des attaques, ou ayant un droit d'usage sur ceux-ci (dans nos exemples des sociétés commerciales, des hôpitaux, des administrations ou des industriels…).
      - La deuxième catégorie est très souvent distincte de cette première et regroupe les victimes indirectes ou par « ricochet »: les clients, utilisateurs, patients, souscripteurs des sociétés en question.

      L'aspect sinistre individuel –sinistre sériel est complexe
    - **La datation est difficile**
      - Des processus dormants
      - Des outils « fire and forget » tels que des virus
    - **La durée de l'événement est indéterminée**
      - La durée de l'événement est parfois impossible à identifier

      (Sa durée et …la durée de ses conséquences)

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **Un risque assurable ? Un risque déjà assuré ?**

L'assurabilité, un sujet complexe: (Un sujet oublié : existence de risque n'implique pas assurabilité.)

- **L'extériorité de la victime face à la survenance de l'événement à garantir est nécessaire.**
- **L'aspect aléatoire est lui aussi clef.**

Exemple: Pour des raisons économiques, ne pas prendre les mesures de protection nécessaire admises comme une norme et / ou un standard et subir une cyber attaque, est ce aléatoire? Pas si sûr.

Assurable économiquement?

- **Il s'agit ici de parler de fonds propres et d'appétit au risque pour des événements corporels, matériels et immatériels pouvant être cumulatifs.**
  - ❖ **Sachant que qu'une partie des sinistres peuvent être de nature corporelle donc de coût unitaire plus important.**

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- Un risque assurable ? Un risque déjà assuré ?
  - **Contrats spécifiques :**
    - Il existe des contrat spécifiques (voir plus loin).
  - **Concernant les contrats existant classiquement, tant pour les risques de particuliers que pour les risques d'entreprises, la prise en compte des conséquences dommageables d'un incident cyber est possible :**
    - Un accident automobile est garanti quel qu'en soit la cause par le contrat auto y compris ceux ayant pour origine le système embarqué (hacké ou non).
    - Un incendie consécutif au piratage d'un objet connecté ou piloté à distance : est-ce exclu ?
    - La RC d'un fabriquant qui transporte dans ses biens (contre son gré) un malware ne sera-t-elle pas engagée?
    - La RC des Mandataires Sociaux d'un CEO qui n'a pas investi suffisamment dans la protection des risques cybers et dont l'entreprise subit une perte de données personnelles sera-t-elle épargnée ?

    Le sujet ici est celui des wordings des contrats . A-t-on exclu le fait générateur de l'« incident Cyber » ?

    <u>Le risque de l'assureur : l'accumulation de toutes ces garanties cachées</u>

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

100% ActuaireS

INSTITUT DES ACTUAIRES

Réglementation et normes

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Point sur la réglementation

- Les entreprises sont soumises à un risque pour elles-mêmes (impact financier, réputationnel et stratégique) et pour la vie privée et les libertés publiques de leurs salariés, clients et fournisseurs.

- Face à la médiatisation des cyber attaques et à la réalité des risques, la réglementation s'est renforcée tous azimuts, avec des obligations pour les entreprises toujours plus strictes de prévention, réaction et notification.

- Ainsi, aux niveaux européen et français, une « avalanche » de textes est parue…depuis la Loi Informatique et Liberté de 1978.

- Mais le respect de la réglementation est la première pierre de la sécurisation.

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Au niveau européen, citons en particulier :

- ✓ Directive 2013/40/UE « Cybercrime »
- ✓ Directive 2015/2366 « Services de paiements II »
- ✓ Directive 2016/943 « Secret des affaires »
- ✓ Directive 2016/1148 « NIS » (Network and Information Security), à transposer en 2018
- ✓ Règlement 2016/679 « RGPD » (Protection des Données Personnelles), mai 2018

Au niveau français, citons en particulier :

- ✓ Loi Informatique et Liberté : 1978 – 2004 : protection des données personnelles
- ✓ Loi de Programmation Militaire (LPM) de 2013
- ✓ Loi sur le Renseignement du 24 juillet 2015
- ✓ Loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement du 3 juin 2016
- ✓ Loi pour une République Numérique du 7 octobre 2016

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Environnement réglementaire

Européen : NIS+ RGPD

Français : Loi Numérique

Obligations de déclaration aux régulateurs :

- Faille SI
- Violation des données a caractère personnel

Augmentation significative des sanctions financières :

Limitées à 150 K€ aujourd'hui, elles peuvent atteindre 3 M€ avec la Loi Numérique et jusque 4% du CA annuel mondial en application du RGPD

Déploiement d'un dispositif technique et organisationnel pour prévenir et gérer le risque

Prévenir :

- Limiter les impacts financiers ou réputationnels en cas d'attaque
- Contrôler les sous-traitants

Gérer :

- Les déclarations obligatoires (en particulier concernant les données personnelles des clients, des fournisseurs et des salariés),
- Les relations avec le régulateur

Etre en conformité :

Sanctions plus lourdes en cas d'insuffisance du dispositif ou des déclarations

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Vers une quintuple peine pour l'entreprise en cas de piratage...

1. Toutes les conséquences négatives « classiques » liées au piratage (pertes, efforts de remédiation, indisponibilité, effets d'image, procès, etc.).

2. En cas de données personnelles accédées, risque CNIL de constatation d'un défaut de sécurité (à terme, notification obligatoire à la CNIL, voire aux personnes concernées).

3. Si un défaut de sécurité a permis le piratage, diminution des dommages-intérêts en conséquence + nouvelle notification aux personnes !

4. Risques de sanctions diverses (pénales ? A terme surtout 2 % CA mondial + notation financière en berne).

5. Actions de groupe rendues possible contre l'entreprise, du fait des manquements.

Avec l'aimable autorisation du cabinet : ATiPiC AVOCAT — Technologies Informations Propriété Intellectuelle Commerce

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

• Normes : outils de prévention et de sécurisation

Parmi les nombreuses normes (spécialisées ou plus générales):

- **PCI-DSS :** spécialisées sur les données bancaires
- **RGS :** à destination des autorités administratives françaises
- **AIR** : standards de protection, d'organisation et transfert des données
- **ISO 27001 à 27005** : mise en place et gestion d'une politique de sécurité de l'information par une approche de gestion des risques
- **SSAE 16 :** attestation de la réalité des contrôles (intégrité de l'information)
- **Les recommandations de l'ANSSI** (Agence Nationale de la Sécurité des SI)

L'application des normes peut faire l'objet d'une certification par un tiers.

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Les acteurs de place

Au niveau Européen, citons en particulier :

- **L'ENISA :** chargé de coordonner l'implémentation des politiques de sécurité au niveau européen et de développer une culture de la sécurité des réseaux d'information dans toute l'Union Européenne.

Au niveau français, citons en particulier :

- **L'ANSSI:** en charge de la sécurité des réseaux et systèmes IT *(NIS)*
- **La CNIL**: protection de l'intégrité des données personnelles et de la protection des libertés individuelles *(Loi Numérique et RGPD)*
- **Le CERT-FR**: détection des vulnérabilités, pilotage de la résolution des incidents et aide à la mise en place de moyens de prévention
- **L'ARCEP,** dans le domaine des Télécommunications
- **L'ACPR et l'AMF** dans le domaine Assurance, Banque, Finance

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

La gouvernance interne aux entreprises

Le dispositif interne s'appuie sur deux acteurs :

- Le Correspondant Informatique et Liberté **(CIL)**
- Le Responsable de la Sécurité des Systèmes d'Informations **(RSSI)**

La fonction de Data Protection Officer (DPO) va s'imposer et se structurer au vu des exigences réglementaires (loi Numérique, RGPD)

La Politique de Sécurité du SI (PSSI) est le document « chapeau » :

- Elle se décline en Directives, Chartes, Procédures, Bonnes pratiques.
- Elles sont transversales : Techniques, Juridiques, Conformité, RH.
- Elles doivent faire l'objet de sensibilisation régulière.
- Leur respect est intégré dans le programme de Contrôle Interne.

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

De l'audit des risques à la maîtrise des risques

- **Le respect des réglementations et des normes** permet de prévenir, dans une certaine mesure, les cyber-attaques et de limiter leur impact.
- **La certification de l'application des normes** est davantage une mise en conformité qu'une évaluation du niveau de risque de sécurité du SI.
- **L'audit des risques de SI** par un cabinet spécialisé permet d'évaluer un niveau de sécurité du SI de l'entreprise.
- Mais la **difficulté d'évaluer/quantifier ce type de risque** rend son pilotage difficile par les dirigeants des entreprises, sur un domaine technique.
- **La difficulté d'estimer le risque résiduel** donne donc des perspectives de transfert de risque propices aux offres assurantielles.
- Pour les assureurs, l'évaluation de ce **risque opérationnel majeur** doit s'inscrire dans la modélisation du risque opérationnel au sein de Solvency II

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Transfert du risque : Etat des lieux du marché

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **L'offre actuelle**

Les attentes des entreprises

- Une assistance rapide
- Un conseil juridique

Les leviers commerciaux

- Notification légale en cas de vol de données personnelles
- Peur de l'évènement majeur

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

• Tendance du marché

Une avance des USA

- Une législation plus mature et plus contraignante (en particulier sur l'obligation de notification)
  - ❖ Hausse des coûts des événements cyber (notification, investigation, défense, indemnisation)
  - ❖ Besoin d'assurance accru
  - ❖ Développement du marché de l'assurance
- Une offre plus mature
- Des données publiques

Un marché en pleine expansion

- De nombreux acteurs spécialisés et généralistes (Beazley, Hiscox, AXA, Allianz…)
- Arrivée d'assureurs généralistes ciblant les TPE (GAN)

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

100% ActuaireS

INSTITUT DES ACTUAIRES

Mesure et gestion du risque

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- Mesure du risque

Problématique d'assurabilité : mesure du risque

- Manque de données -> modèles actuariels classiques non adaptés
- Difficulté à tarifer et à différencier le risque

Les principaux critères de différenciation reposent sur les caractéristiques de l'entreprise assurée :

- Secteur d'activité
- Données spécifiques de l'entreprise (taille, chiffre d'affaires,…)
- Indicateurs d'exposition (nature des données traitées, dépendance aux réseaux, externalisation, sécurité des SI, …)
- Type de couverture (dommages / RC) et nature des garanties ;
- Réglementation et juridiction locale

Axes de développement : scoring et analyse prédictive

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- Gestion des accumulations
  - **Evaluation de l'appétit au risque cyber**
    - Détermination des limites au risque cyber.
  - **Cartographie du risque**
    - Identification des polices et des garanties (implicite et explicite) sujettes au risque.
    - Identification des expositions.
      - ❖ Problématique : quelle mesure adopter ?
    - Déterminer les niveaux de PML (Probable Maximum Loss)
      - ❖ Problématique : difficile compte tenu du peu d'historique de sinistres
        - Recours à des avis d'expert.
        - Utilisation de scénarios stressés sur le portefeuille.
        - Taux de perte observés sur d'autres branches de risques.

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Atténuation du risque

Limites de garanties

- Limite le marché car en dessous du PML

Normes et audits

- Les normes sensibilisent les petites structures
- Les audits (grosses structures)

Réassurance

- Acteurs traditionnels
- Insurance Linked Securities (appel au marché)

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Conclusion : l'actuaire et le risque cyber

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **L'actuaire et le risque cyber**
  - **Quels métiers concernés ?**
  - **Quelles problématiques opérationnelles ?**
  - **Quelles solutions ?**
  - **Conclusion**

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **Du point de vue de l'assureur / réassureur**
  - **Le risque cyber est souscrit par la compagnie**
    - Une **garantie** offerte par l'assureur dont il faut définir l'étendue, le prix et provisionner le coût
      - ❖ Concerne l'actuaire Produit et l'actuaire Réserves
    - Un **risque d'assurance** émergent à identifier, quantifier, piloter et réduire
      - ❖ Concerne l'actuaire Insurance Risk Manager

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **Du point de vue de l'entreprise (y compris sociétés d'assurance et de réassurance)**

Le risque cyber est porté par l'entreprise

- Un **risque opérationnel** propre à identifier, quantifier, piloter et réduire
  - ❖ Concerne l'actuaire Operational Risk Manager ou ERM
  - ❖ Exemple : rapport Airbus sur la maîtrise du risque Cyber et Assurance avec la participation de l'Institut des Actuaires

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **Le sujet des données**

Information interne

- Identifier et enregistrer les sinistres / incidents (« flags »)
- Evaluer et surveiller l'exposition et les cumuls
  - ❖ Problème : identification des engagements « cachés », dimension temporelle

Information marché

- Collecter les informations sur les sinistres / incidents du marché (local, européen, mondial)
  - ❖ Problème : détail, ventilation entre pertes économiques et pertes assurantielles, pertinence, exhaustivité (secteur, exposition, juridiction, évolutivité)

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

- **Les outils et solutions à disposition de l'actuaire pour évaluer et gérer le risque cyber**
  - **Les techniques d'approches par scenarii**
  - **Des systèmes internes efficaces de reporting et de suivi des risques**
  - **Une communication des enjeux au top management**
  - **Comme pour les risques spéciaux, une interaction constructive avec les experts du risque de sécurité informatique ainsi qu'avec les juristes et experts sinistres**
  - **Une collaboration avec les acteurs qui ont une vision marché de ce risque (réassureurs, consultants, courtiers) et des moyens de le couvrir**

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

Conclusion : une opportunité pour le métier d'actuaire

Positionnement stratégique à la croisée des métiers IT/juridique/financier

- Coordonne, promeut et influence tant dans le domaine de la collecte des données que dans celui du respect des normes et du cadre réglementaire.
- Renforce et améliore les techniques d'évaluation et de suivi du risque, dans un contexte prudentiel très contraignant.

Positionnement éthique, dans une recherche d'équilibre raisonné entre technologie et humanité

- Exerce son rôle en conformité avec le Code de Déontologie de la profession
- Se place comme le garant de la donnée et aussi des algorithmes

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com

MERCI POUR VOTRE ATTENTION

Des questions ?

4, rue Chauveau-Lagarde - 75008 Paris - Tél : 01 44 51 72 72 - Fax : 01 44 51 72 73
www.institutdesactuaires.com