L’ASSURANCE CYBER, COMMENT ASSURER LE RISQUE ?

ADSTO
Avocats à la Cour

CLEVER COURTAGE
IT Risk Insurance Broker

Fédération Française de l’Assurance

ADSTO
Avocats à la Cour

Déroulement de l'intervention

Intervention de C. BERNIER– le rôle de l'avocat

La connaissance de l'exposition au cyber risque et de sa couverture

Intervention de C. DELCAMP

Introduction :
La diversité des risques et leurs conséquences
Définition et caractéristiques du risque cyber

La vie du contrat

Intervention de C. DELCAMP

Le transfert du cyber risque à l'assurance

Gestion de la crise

Intervention de JL. SANTONI

Modèles d'offres possibles sur le marché

Intervention de JL. SANTONI

Exemples concrets : Saint Gobain, Centre Marie Curie, Hertz, Darty ..

La diversité des risques cyber
Une prise de conscience des assureurs

Fédération Française de l'Assurance

CHIFFRES CLÉS DE LA FFA

99 %
des sociétés d'assurances en France

1er
marché de l'Union européenne post Brexit
et **5ème** mondial

37 millions
de bénéficiaires d'une assurance vie

2,1 millions
d'entreprises assurées

146 200
salariés du secteur

280
entreprises membres

40 millions
de contrats habitation

42 millions
de véhicules assurés

13,4 millions
de sinistres gérés par an

170
collaborateurs

Fédération Française de l'Assurance

EQUIFAX

Septembre 2017

Janvier 2018

Janvier 2018

Juillet 2016

Deloitte.

De novembre 2016 à avril 2017

Avril 2017

OVH.com

Septembre 2016

SONY

Novembre 2014

Commission européenne

Novembre 2016

TV5MONDE

Avril 2015

TARGET

Décembre 2013

NETFLIX

Spotify

BANGLADESH BANK

Avril 2016

elysee.fr

Mai 2012

STUXnet

Dès 2007

YAHOO!

Aout 2013

PayPal

Octobre 2016

Dec 2014

Les attaques cyber concernent également les assureurs, les administrations, les TPE et PME …

Fédération Française de l'Assurance

A l'origine de ces deux virus, il y a des déclinaisons des outils de la NSA

WannaCry, considéré comme le plus grand piratage à rançon de l'histoire d'Internet, a frappé en mai et juin 2017 et infecté plus de **300 000 ordinateurs dans plus de 150 pays,** affectant notamment le système de santé britannique, les chemins de fer allemands ou des usines Renault en France

NotPetya, en juin 2017, était en revanche une **attaque en sabotage** : le logiciel malveillant a effacé les fichiers des ordinateurs qu'il visitait, se faisant passer pour un *ransomware.* La majorité des entreprises visées étaient situées en Ukraine mais **les dégâts sont mondiaux** : la principale victime française connue est le groupe de matériaux de construction Saint-Gobain, qui évalue le manque à gagner à 250 millions d'euros

http://www.lemonde.fr/ameriques/video/2017/04/10/dallas-des-pirates-informatiques-declenchent-toutes-les-sirenes-d-alarme-de-la-ville-en-pleine-nuit_5109046_3222.html

Cyber Espionnage	• Etatique • Politique • Industriel
Cyber Vol	• Ciblée
Cyber divulgation	• Atteinte à l'image de marque
Cyber Extorsion	• Ciblée • **Massive**

Cyber SABOTAGE	• Ciblé • Massif

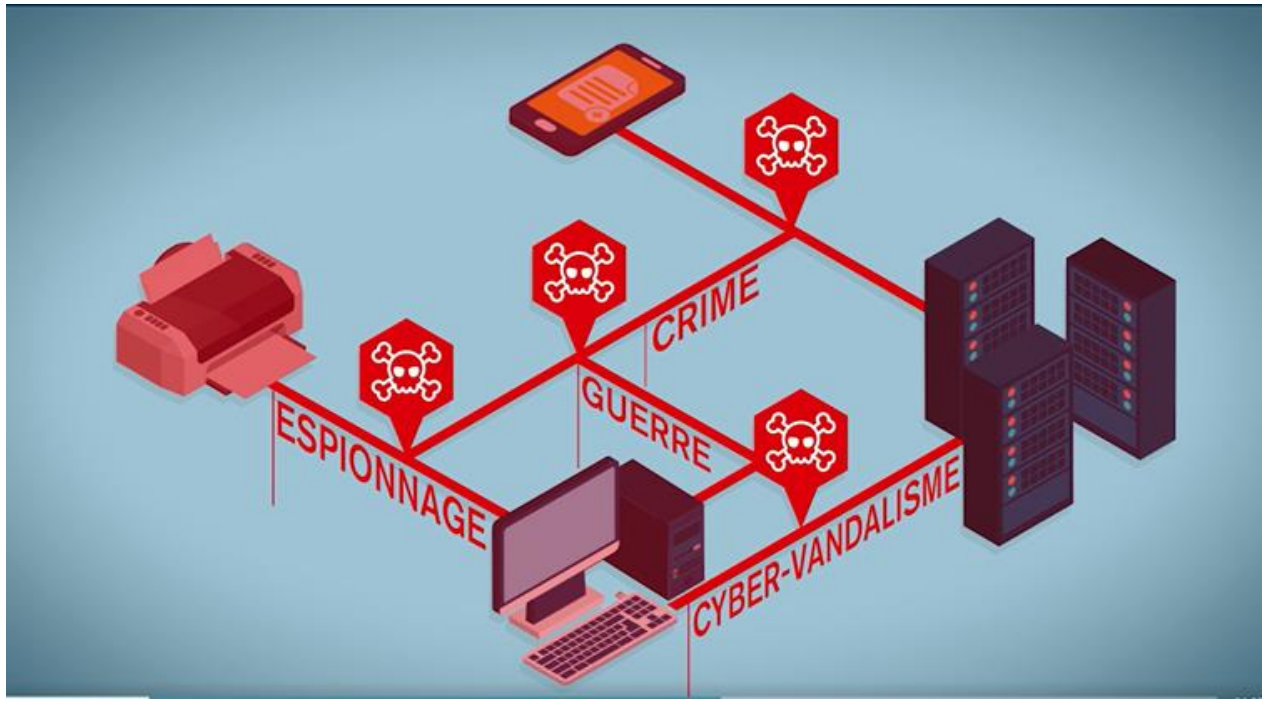
Fédération Française de l'Assurance

Un développement sans conscience du risque

Espace privé l'entreprise

Espace public

Espace privé personnel



Fédération Française de l'Assurance

Les conséquences sur les grands groupes

L'exemple d'Equifax

7 septembre 2017

142.7 USD cours de l'action de l'action Equifax

Annonce du piratage du système informatique Vol des données de 145 millions d'américains

8 septembre

123.23 cours de l'action
perte de 14%

15 septembre

92,92 USD cours de l'action
perte de 35%

Licenciement du responsable de la sécurité et du directeur informatique

Cours de l'action commence à remonter

22 septembre

Démission du C.E.O. d'Equifax

Source Boursorama 03/10/2017

Fédération Française de l'Assurance

Définitions et caractéristiques du risque cyber

Définition du risque cyber

Le risque cyber, pour une entreprise, c'est la probabilité que se produise un événement, qui vient :

- ✓ Altérer l'intégrité ou la confidentialité du système d'information de l'entreprise.
- ✓ Corrompre, effacer ou rendre public des données que l'entreprise héberge.

Les faits générateurs

Le risque cyber pour une entreprise c'est la probabilité que se produise un événement, généré par :

- ✓ Actes Malveillants
- ✓ Erreurs humaines

Les Risques

- ✓ Espionnage
- ✓ Vol
- ✓ Divulgation
- ✓ Sabotage
- ✓ Extorsion

Les conséquences dommageables

- ✓ Pertes financières directes et indirectes
  - ➢ Frais de notification
  - ➢ Payement d'une rançon
  - ➢ Amendes
  - ➢ Gestion de crise - Forensic
  - ➢ Reconstitution de données

- ✓ Pertes immatériels liées notamment à l'atteinte à l'image de marque de l'entreprise

Caractéristiques du risque Cyber

Des risques multiples, évolutifs, difficilement maitrisables et encore sous estimés :

Des compétences informatiques vulgarisées :

- ✓ Scientifiques
- ✓ R&D
- ✓ Etudiants informatiques
- ✓ Geek

Caractéristiques du risque Cyber

Des acteurs multiples:

- ✓ Etats
- ✓ Activistes
- ✓ Entreprises
- ✓ Criminels

Caractéristiques du risque Cyber

Un développement technologique vecteur de risque

- ✓ BYOD
- ✓ Réseaux sociaux
- ✓ Objets connectés
- ✓ Interconnexion des réseaux
- ✓ Développement du cloud
- ✓ Big Data

Caractéristiques du risque Cyber

Des espaces abrogés

- ✓ TEMPS
- ✓ GEOGRAPHIQUES

ADSTO
Avocats à la Cour

L'intervention de l'avocat dans le transfert du cyber risque de l'Entreprise à l'assurance

Souscription du contrat

1. **Programme de conformité** *(cartographie des risques notamment sur les données et les SI)*
2. **Sensibilisation à la vulnérabilité** de l'entreprise face aux cyber risques
3. **Analyse des contrats déjà souscrits** *(garanties et clauses d'exclusion)*
4. **Négociation du contrat de cyber assurance** *(garanties, clauses d'exclusion et primes)*

Les interlocuteurs de l'Avocat :

- Organes dirigeants de l'Entreprise
- Risk manager / Compliance Officer
- Courtier
- Assureur

Le transfert du risque cyber à l'assurance

Les garanties proposées par l'assurance
pour faire face aux cyber attaques

Fédération Française de l'Assurance

A. L'évaluation de l'exposition au risque cyber

B. L'analyse du risque cyber

C. Les garanties existantes

1. Dans les contrats Cyber purs
2. Dans les contrats de Responsabilité Civile
3. Dans les contrats de Dommage aux Biens

L'évaluation de l'exposition au risque et de la quantification financière

Il est impératif :

- d'identifier les facteurs de risque (surface d'attaque & attractivité)
- de faire une évaluation relative

Suivant les réglementations ou les exigences contractuelles :

- RGPD
- Données médicales
- NIS

En fonction de son activité :

- Secteur Industriel
- Vente et Commerce
- Logistique
- Opérateur de réseau
- Fournisseur de service tangible
- Fournisseur de service intangible

Selon la maniére dont son entreprise utilise les outils informatiques :

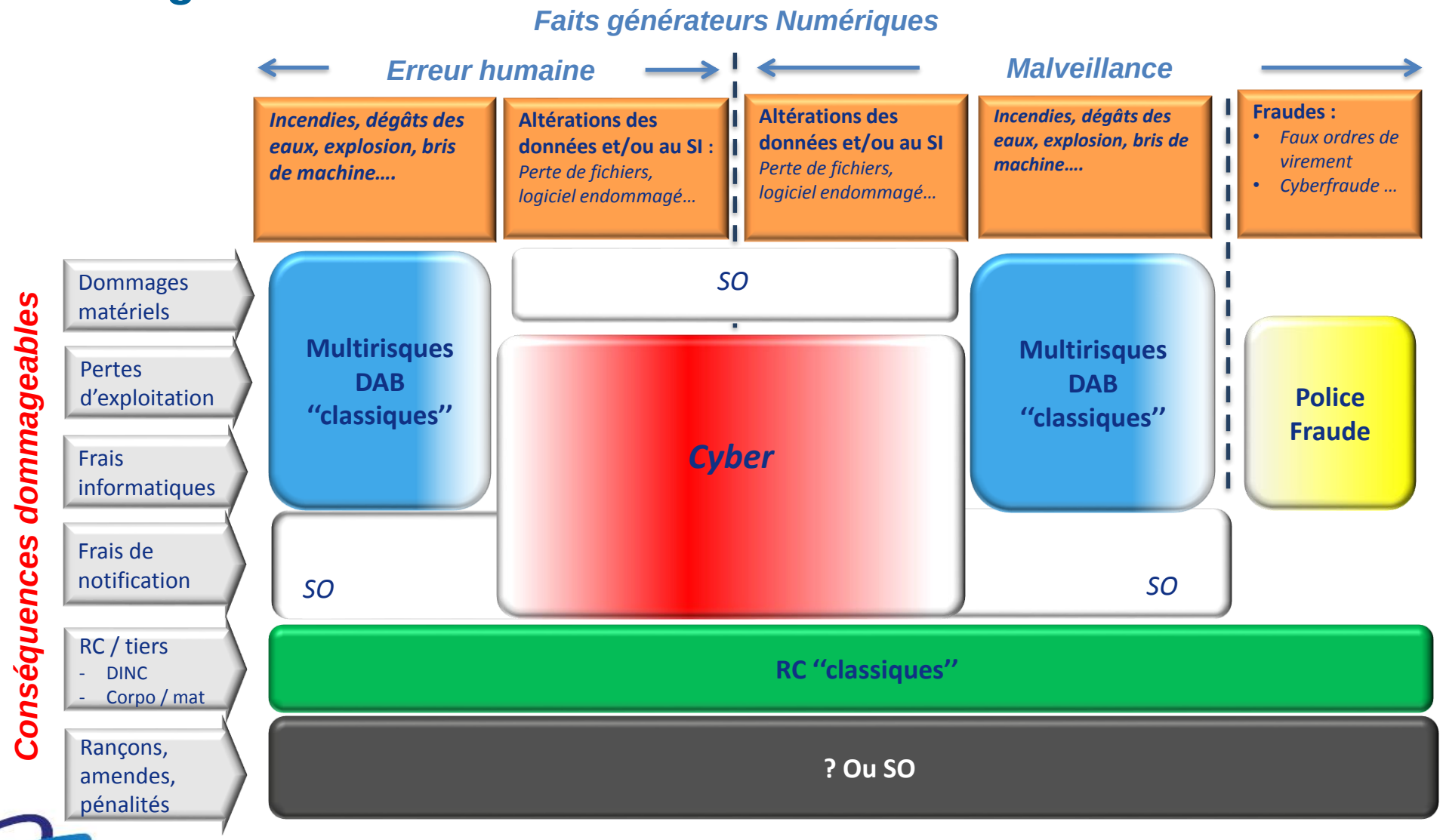
- Pour les activités support (compta, achats, RH, gestion clients, …)
- Pour les activités opérationnelles métiers (fabrication, R&D, gestion des stocks, logistique, …)
- Pour les produits et/ou services fournis

Les garanties existantes

Le risque cyber peut être couvert par plusieurs types de garanties que l'on retrouve :

- ✓ Dans les contrats cyber
- ✓ Dans les contrats de Dommage aux biens
- ✓ Dans les contrats de Responsabilité civile

Les garanties existantes



Les problématiques en cours

Le risque cyber génère de nouveaux enjeux liés:

- ✓ Aux Silent Covers
- ✓ A l'assurabilité:
  - ✓ Des Rançons
  - ✓ Des amendes

ADSTO
Avocats à la Cour

L'intervention de l'avocat dans le transfert du cyber risque de l'Entreprise à l'assurance

Souscription du contrat

1. **Programme de conformité** *(cartographie des risques notamment sur les données et les SI)*
2. **Sensibilisation à la vulnérabilité** de l'entreprise face aux cyber risques
3. **Analyse des contrats déjà souscrits** *(garanties et clauses d'exclusion)*
4. **Négociation du contrat de cyber assurance** *(garanties, clauses d'exclusion et primes)*

1. **Pérennisation de la conformité de l'Entreprise** aux exigences de la réglementation (*registres de traitements, mesures de sécurité...)*
2. **Renégociations ponctuelles des contrats d'assurance**, en déclarant les évolutions favorables à la diminution de l'exposition au cyber risque

Les interlocuteurs de l'Avocat :

- Organes dirigeants de l'Entreprise
- Risk manager / Compliance Officer
- Courtier
- Assureur

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur la mise en place de programme d'assurance Cyber à vocation de masse :

- exemple d'approche dédiée sous forme de gamme : produits Pro - TPE Standard et produit Sur Mesure
- exemple d'approche intégrée sous forme d'extension Cyber dans une police Groupe RCPro

Jean Laurent SANTONI
Docteur en Droit, depuis 35 ans dans le domaine de l'assurance des risques informatiques,
Il réalise des missions d'expertises, d'audit et de conseils auprès d'Institutions, d'assureurs, de réassureurs, de captives d'assurance et de réassurance, et au bénéfice de Directions Générales qui recherchent son expertise, sa séniorité et son indépendance.

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur la mise en place de programme Cyber

Le challenge : participer à l'élaboration pour le réseau d'agents d'un assureur généraliste d'une offre Cyber simple à vendre, facile à souscrire et à l'indemnisation efficace.

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur la mise en place de programme Cyber

Une gamme Cyber correspondant aux besoins

OFFRE STANDARD

- Offre dédiée aux entreprises et professionnels réalisant moins de 1 Millions d'€ de CA
- Pas de questionnaire de souscription – un contrat simple et facile à comprendre
- Prise de garantie immédiate : dés que le bulletin de souscription est complété, signé et daté
- Une plate-forme pour porter assistance car le plus important est d'aider l'assuré à gérer et surmonter la crise
- Un accès à un réseau maillé France entière d'experts en sécurité informatique, avocats et experts judiciaires
- Un assureur Français avec son centre de décision en France et une politique de gestion des sinistres en France avec des acteurs Français

Volet RC

- Conséquences d'une violation de la législation sur la protection des données personnelles
- Conséquences d'une atteinte à la confidentialité des informations
- Conséquences d'une atteinte du SI ou des données d'un tiers via le SI de l'assuré (y compris les conséquences d'une transmission de virus à des systèmes tiers)
- Frais de défense

Volet Gestion de crise

- Qualification de la situation
  - Coûts d'investigations et d'enquêtes
  - Frais de consultant en sécurité informatique (qualification de l'évènement)
  - Frais de consultant juridique (qualification du régime d'obligations réglementaires applicables)
- Traitement de la situation
  - Coûts de gestion de la procédure avec les Autorités de contrôle
  - Frais de notification suite à une injonction des Autorités de Contrôle
  - Frais de communication

Volet DB

- Frais de décontamination suite à une atteinte aux données et aux SI (y compris à la suite de virus)
- Frais de reconstitution des données et frais de restauration des sauvegardes suite à une atteinte aux données et aux SI
- Frais supplémentaires d'exploitation suite à une atteinte aux données et aux SI

Capital gestion de crise 50.000 €
Capital combiné RC Dommages 100.000 €
Total 150.000 €

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur la mise en place de programme Cyber

Une gamme Cyber correspondant aux besoins

OFFRE SUR MESURE

- Offre dédiée aux entreprises et professionnels quel que soit leur CA pour des garanties cumulées jusqu'à 1 Million d'€
- Un questionnaire de profilage simple à compléter – une aide à la vente
- Une offre complète avec des options adaptées à tous les types de clients
- Un accès à une capacité importante si nécessaire

Volet RC

- Les garanties de l'offre « Standard »
- Mise en cause suite à une atteinte à la propriété intellectuelle ou une atteinte à la vie privée ou du droit à l'image
- Mise en cause suite à agissement diffamatoire, publicité mensongère ou dénigrement

Volet Gestion de crise

- Qualification de la situation
  - Coûts d'investigations et d'enquêtes
  - Frais de consultant en sécurité informatique (qualification de l'évènement)
  - Frais de consultant juridique (qualification du régime d'obligations réglementaires applicables)
- Traitement de la situation
  - Coûts de gestion de la procédure avec les Autorités de contrôle
  - Frais de notification suite à une injonction des Autorités de Contrôle
  - Frais de communication

Volet DB

- Les garanties de l'offre « Standard »
- Frais de reconstitution des données et frais de restauration des sauvegardes suite à une atteinte aux données et aux SI suite y compris si la cause est une erreur humaine
- Pertes d'exploitation suite à une atteinte aux données et aux SI de l'Assuré
- Frais et dépenses suite à une cyber extorsion
- Pertes financières de l'assuré liée à une fraude liée à une défaillance de sécurité informatique

Capital gestion de crise à définir
Maintien d'une approche par capital combiné RC Dommages
Ou dissociation des capitaux RC Dommages

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur la mise en place de programme Cyber

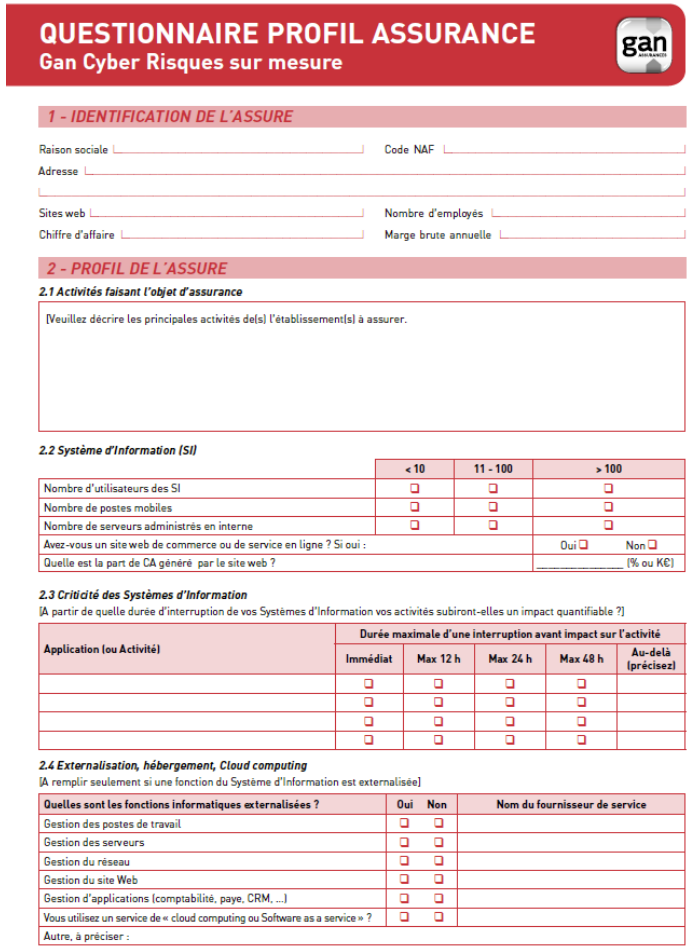
Des conditions de souscription simplifiées

Processus de souscription		Gamme		
		Standard	Sur-mesure	Fac ou acceptation spéciale
Conditions d'octroi de la garantie en cas de sinistre - mesures préventives à respecter - devoir de conseil du souscripteur à la signature de la police	Back-up	Oui	Oui	Oui
	Anti-virus	Oui	Oui	Oui
	Pare-feu	Oui	Oui	Oui
	Test de logiciel	Non	A évaluer à travers le questionnaire	A évaluer à travers le questionnaire
	Plan de secours	Non	A évaluer à travers le questionnaire	A évaluer à travers le questionnaire

Les conditions d'octroi de la garantie cyber risques reposent sur les recommandations de l'ANSSI. Elles sont la traduction assurancielle des bonnes pratiques de sécurité, et sont modulées en fonction de la gamme de garantie souscrite. Ces bonnes pratiques sont exposées dans un guide intitulé « Guide d'Hygiène Informatique » qui est remis à chaque assuré. Ce Guide prévoit au total 40 règles. L'Assureur a choisi de n'en retenir que 3 pour la souscription de la formule standard et d'en rajouter 2 pour la formule sur-mesure. En outre, il est stipulé que la condition d'octroi ne s'exercera toutefois pas s'il s'avère que le dommage est sans relation avec le non- respect de la condition.

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur la mise en place de programme Cyber



QUESTIONNAIRE PROFIL ASSURANCE
Gan Cyber Risques sur mesure

1 - IDENTIFICATION DE L'ASSURE

Raison sociale ____ Code NAF ____
Adresse ____
Sites web ____ Nombre d'employés ____
Chiffre d'affaire ____ Marge brute annuelle ____

2 - PROFIL DE L'ASSURE

2.1 Activités faisant l'objet d'assurance

[Veuillez décrire les principales activités de(s) l'établissement(s) à assurer.

2.2 Système d'Information (SI)

	< 10	11 - 100	> 100
Nombre d'utilisateurs des SI	❑	❑	❑
Nombre de postes mobiles	❑	❑	❑
Nombre de serveurs administrés en interne	❑	❑	❑
Avez-vous un site web de commerce ou de service en ligne ? Si oui :			Oui ❑ Non ❑
Quelle est la part de CA généré par le site web ?			_____ [% ou K€]

2.3 Criticité des Systèmes d'Information

[A partir de quelle durée d'interruption de vos Systèmes d'Information vos activités subiront-elles un impact quantifiable ?]

Application (ou Activité)	Durée maximale d'une interruption avant impact sur l'activité				
	Immédiat	Max 12 h	Max 24 h	Max 48 h	Au-delà (précisez)
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	

2.4 Externalisation, hébergement, Cloud computing

[A remplir seulement si une fonction du Système d'Information est externalisée]

Quelles sont les fonctions informatiques externalisées ?	Oui	Non	Nom du fournisseur de service
Gestion des postes de travail	❑	❑	
Gestion des serveurs	❑	❑	
Gestion du réseau	❑	❑	
Gestion du site Web	❑	❑	
Gestion d'applications (comptabilité, paye, CRM, ...)	❑	❑	
Vous utilisez un service de « cloud computing ou Software as a service » ?	❑	❑	
Autre, à préciser :			

1

Focus sur l'approche Profilage

Le questionnaire a été construit afin de répondre à trois objectifs :

- Evaluer l'exposition aux risques de l'Assuré afin de déterminer le niveau de tarification applicable
- Evaluer l'exposition aux risques de l'Assuré pour identifier les garanties correspondantes à ses besoins de couverture.
- Permettre un traitement « Big Data » des profils pour identifier les risques de cumuls et de sériels liés aux technologies et aux prestataires similaires

La tarification prend en compte les éléments suivants :

L'activité (description et code NAF)

- Le chiffre d'affaires
- Le niveau de franchise choisi
- Le nombre d'enregistrements de données détenus pour l'activité de l'assuré
- Le niveau de qualité du risque en fonction des réponses positives aux questions « Politique de Sécurité des Systèmes d'Information (PSSI) »,

Une base « Big Data » de profilage et de cumul d'exposition a été élaboré avec la plateforme Cybex Assistance.

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur la mise en place de programme Cyber

Une indemnisation efficace via une plateforme de gestion de crise et de sinistre

La prise en charge d'une cyber attaque se caractérise par trois phases :

- La crise : c'est la phase de réaction à chaud : l'objectif est le retour en service pour les utilisateurs (internes et externes). Cette phase démarre à la détection de l'attaque et se termine lors de la restauration du service. Cette phase peut être très courte, voire inexistante dans certains cas (par exemple le vol de données qui est transparent pour les utilisateurs)
- La décontamination : c'est la phase d'analyse à froid : l'objectif est le retour à une situation nominale après une analyse de l'origine de l'attaque. Il s'agit généralement de nettoyer, voire de réinstaller les plateformes. Cette phase inclue les recommandations d'actions préventives, pour éviter que la même attaque, ou d'autres, ne se reproduisent.

Il s'agit d'une approche d'urgence

- La recherche de responsabilités : cette phase démarre en parallèle de la phase de crise, notamment par la recherche et la préservation des preuves. L'objectif est d'indemniser les préjudices et de se donner les moyens d'un recours ultérieur envers les cyber attaquants et/ou envers les tiers concernés (fournisseurs, hébergeurs, infogérants, …).

Il s'agit d'une approche plus classique des experts d'assurance

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur la mise en place de programme d'assurance Cyber à vocation de masse :

- exemple d'approche intégrée sous forme d'extension Cyber dans une police Groupe RCPro

La police Groupe RCPro des Experts-comptables

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur la mise en place de programme Cyber

La police Groupe RCPro des Experts-comptables

Garantie intégrée dans la police Groupe RCPro des Experts-comptables

RCP n° 118 269 730 :

- gestion de crise à hauteur de 50 000 € avec franchise de 300 € ;
- pertes de données à hauteur de 120 000 € sans franchise ;
- frais supplémentaires d'exploitation / frais de notification / fraude / cyber extorsion à hauteur de 20 000 € avec franchise de 1 800 € portée à 5 400 € en cas de non-respect des mesures de prévention.

CONDITIONS DE GARANTIE

Les garanties ne seront accordées que si les mesures de prévention suivantes sont respectées :

a. la connexion au réseau informatique ou au poste informatique se fait via un mot de passe contenant au minimum 8 caractères,
b. les Logiciels et applications utilisées, lorsqu'ils sont mis à jour, le sont suivant les recommandations de l'éditeur,
c. un anti-virus et un firewall sont installés sur le système d'information et mis à jour automatiquement,
d. une sauvegarde au minimum hebdomadaire des données informatiques est réalisée sur des supports externes et stockés à l'extérieur de l'établissement,
e. les employés des cabinets d'expertises-comptables sont sensibilisés aux risques et menaces liées aux cyberattaques.

L'assuré déclare avoir pris note des recommandations suivantes :

a. lors de l'utilisation de la messagerie, ne pas ouvrir de pièces jointes ou de lien provenant de destinataire inconnu ou dont le titre ou le format paraissent incohérent. Les pièces jointes ne doivent pas comporter de format du type .com / .exe / .vbs / .lnk / etc.
b. un paiement sur internet ne doit se faire que si la mention « https:// » apparaît au début de l'adresse du site internet,
c. lors d'un déplacement les appareils et supports doivent être gardés avec son propriétaire et/ou utilisateur pour éviter le risque de vol,
d. les ordinateurs portables doivent disposer d'un système de chiffrement intégral permettant de sécuriser le disque dur.
e. dans le cas d'un prestataire cloud les recommandations du conseil supérieur de l'ordre des experts-comptables « conformite cloud 2016 » seront appliquées.

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur la mise en place de programme Cyber

La police Groupe RCPro des Experts-comptables

ASSURANCE 2ème LIGNE

Option 1 avec cotisation annuelle de 221 € TTC

GARANTIES OPTION 1	MONTANT
Gestion de crise Pertes de données Frais sup d'exploitation Frais de notification Fraude Cyber extorsion	50 000 € limité à 25 000 € pour la garantie fraude limité à 25 000 € pour la garantie cyber extorsion

Option 2 avec cotisation annuelle de 439 € TTC

GARANTIES OPTION 2	MONTANT
Gestion de crise Pertes de données Frais sup d'exploitation Frais de notification Fraude Cyber extorsion	100 000 € limité à 50 000 € pour la garantie fraude limité à 50 000 € pour la garantie cyber extorsion

Option 3 avec cotisation annuelle de 615 € TTC

GARANTIES OPTION 3	MONTANT
Gestion de crise Pertes de données Frais sup d'exploitation Frais de notification Fraude Cyber extorsion	200 000 € limité à 75 000 € pour la garantie fraude limité à 75 000 € pour la garantie cyber extorsion

Il est rappelé que quelle que soit la nature des garanties engagées, le montant maximum des garanties complémentaires ne dépassera pas 50 000 € en option 1 100 000 € en option 2 et 200 000 € en option 3 par sinistre et par année d'assurance.

CLEVER COURTAGE
IT Risk Insurance Broker

Garantie cyber intégrée ou garantie dédiée ?

L'ensemble du Marché s'est prononcé en faveur des garanties Cyber dédiées et nous avons montré que l'on pouvait proposer des garanties dimensionnées pour apporter une réponse adaptée qui passe principalement par une garantie de Gestion de Crise dont l'efficacité permet de limiter l'exposition en Dommages ou en RC par la bonne qualification de la situation et une réponse rapide adéquate.

Les garanties Cyber intégrées dans une police Dommages (extension atteintes aux systèmes et aux données pour une cause immatérielle) ou Responsabilité Civile Professionnelle (extension aux réclamations des tiers lésés résultant d'une atteinte aux systèmes et aux données) ont le mérite de proposer une garantie élargie, souvent en pollicitation des garanties existantes.

Tout en donnant à l'Assuré un début de commencement d'assurance Cyber, nécessairement limitée en termes de garanties et de capitaux, l'intégration permet à l'Assureur de maitriser son exposition, de recueillir une prime complémentaire et de se protéger contre le risque d'une interprétation extensive de la Police de base si elle n'est pas suffisamment précise (silent cover).

CLEVER COURTAGE
IT Risk Insurance Broker

Quel référentiel de souscription et de suivi des engagements et des expositions ?

Trois hypothèses sont envisageable :

- La simplification de souscription des risques cyber « simple » avec l'absence de questionnaire et le développement de conditions d'octroi de la garantie basées sur les bonnes pratiques de sécurité ;

- La substitution au questionnaire classique sur la description du système informatique assuré d'un questionnaire de profilage « business » à partir duquel on peut construire des familles de profil Utilisateurs / Architectures de Sécurité / Métiers, intégrant des informations relatives aux systèmes dépendants (opérateurs télécoms, fournisseurs de services, technologies partagées, …).

- La mise en place d'une nouvelle branche d'assurance spécifique aux risques cyber pour permettre à la Place et au Régulateur d'évaluer l'exposition au risque, la consolidation de ces informations dans une base de connaissance partagée par les Assureurs et Réassureurs pourrait conduire à identifier les agrégations de risques et l'exposition systémique.

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE
DGSI

INGERENCE ECONOMIQUE

Flash n° 26 - Septembre 2016

ATTENTION :
Si le recours aux assurances est indispensable pour la pérennité de l'entreprise, notamment face à la montée de risques émergents, il convient de s'assurer du respect de la confidentialité des échanges et des données transmises.

ADSTO
Avocats à la Cour

L'intervention de l'avocat dans le transfert du cyber risque de l'Entreprise à l'assurance

Souscription du contrat

1. **Programme de conformité** *(cartographie des risques notamment sur les données et les SI)*
2. **Sensibilisation à la vulnérabilité** de l'entreprise face aux cyber risques
3. **Analyse des contrats déjà souscrits** *(garanties et clauses d'exclusion)*
4. **Négociation du contrat de cyber assurance** *(garanties, clauses d'exclusion et primes)*

Pérennisation du contrat

1. **Pérennisation de la conformité de l'Entreprise** aux exigences de la réglementation (*registres de traitements, mesures de sécurité...)*
2. **Renégociations ponctuelles des contrats d'assurance**, en déclarant les évolutions favorables à la diminution de l'exposition au cyber risque

Contrôle / Enquête de la CNIL
Cyber attaque / Erreur humaine
Non respect de la réglementation

1. **Gestion immédiate de la crise** (*cristallisation des éléments de preuves en cas d'attaque…)*
2. **Participation aux actions de la cellule de crise** *(contact avec les assurances, notification à la CNIL, conseils en matière de communication…)*
3. **Gestion juridique de la crise** *(protection des intérêts de l'entreprise vis-à-vis des tiers – CNIL, assureurs, particuliers)*

Les interlocuteurs de l'Avocat :

- Organes dirigeants de l'Entreprise
- Risk manager / Compliance Officer
- Courtier
- Assureur

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur les sinistres Cyber

Centre Marie Curie IMR

Le Centre Marie Curie a pris en charge, en 2014, 1 468 patients pour délivrer un total de 31 200 séances de radiothérapie. La radiothérapie est une technique de traitement des cancers consistant à exposer le patient à un rayonnement X. L'efficacité de ce type de traitement repose sur un subtil équilibre entre la dose délivrée aux volumes cibles et la dose reçue de manière incidentelle sur les organes de voisinage. Pour des raisons radiobiologiques, la dose totale d'irradiation doit être fractionnée et délivrée de manière quotidienne, 5 jours par semaine, 52 semaines par an. Les interruptions intempestives peuvent compromettre les chances de guérison et d'efficacité des traitements. Entre 110 et 150 patients sont traités chaque jour au Centre Marie Curie.

Le 1er Mai 2015, une intrusion dans le serveur par un compte utilisateur inconnu a provoqué l'effacement de deux disques réseau comprenant la base de données patients et des dosimétries patients sauvegardées sur serveur principal ainsi que la suppression de tous les comptes utilisateurs. L'évènement ayant eu lieu un jour férié suivi d'un week-end, les dégâts n'ont pu être constatés que 3 jours après, le lundi 4 mai au matin, ce qui a empêché de remonter suffisamment loin dans le journal du pare-feu pour analyser de quelle manière le compte inconnu a procédé. Vraisemblablement, un hacker a utilisé un port RDP ouvert sur le routeur permettant à n'importe qui d'extérieur de s'infiltrer dans le réseau du Centre Marie Curie.

Réactions immédiates :
Une interruption de 24 heures a été nécessaire pour charger les disques de sauvegarde (sauvegarde externalisée sur disques optiques). Vingt-quatre heures supplémentaires ont été nécessaires pour restaurer les serveurs permettant de reprendre le travail de dosimétrie. Des doutes restent sur la restitution ad integrum de l'ensemble des bases de données.

Intervention de l'assurance :
Le Centre Marie Curie n'avait pas souscrit de garantie d'assurance cyber risques. **Pour autant les préjudices corporels sont exclus.**
La question de l'applicabilité de la police d'assurance de responsabilité civile médicale a été posée.

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur les sinistres Cyber

220 millions d'euros de chiffre d'affaires. C'est ce qu'a perdu Saint Gobain lors de l'attaque cyber NotPetya en juin 2017. A l'occasion des rencontres annuelles de l'AMRAE qui se sont tenues du 7 au 9 février 2018, Claude IMAUVEN, directeur opérationnel du groupe est revenu sur les conséquences de cette attaque.

"Il y a un avant et un après l'attaque NotPetya", c'est avec ces mots que Claude IMAUVEN, numéro 2 du groupe français, est revenu sur la cyberattaque, subie par Saint Gobain le 27 juin 2017. "Le virus NotPetya a contaminé les ordinateurs via un logiciel de l'administration fiscale ukrainienne auquel les entreprises doivent se connecter", raconte le dirigeant. En quelques minutes, des milliers de données sont cryptées, impossible à récupérer.

Résultat : des systèmes de commandes et de facturation informatique bloqués. Les réseaux de distribution du groupe, Point P et Lapeyre, ont du revenir au stylo et au papier pour rédiger les bons de commande et les transmettre manuellement. Quatre jours de gestion de crise, 10 pour que l'activité reprenne totalement.

Saint Gobain n'avait pas souscrit d'assurance Cyber. Depuis il l'a fait (mais garde ses conditions d'assurance confidentielles) et exige désormais des fournisseurs que ceux qui se connectent directement au système du groupe soient cyber-vertueux.

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur les sinistres Cyber

En octobre 2016, la CNIL a été informée de l'existence d'un incident de sécurité sur le site « www.cartereduction-hertz.com ». Lors d'un contrôle en ligne elle a constaté que les mesures garantissant la sécurité et la confidentialité des données des adhérents au programme de réduction de la société étaient insuffisantes. En effet, les agents de la CNIL ont pu accéder librement, à partir d'une adresse URL, aux données personnelles renseignées par 35 357 personnes inscrites sur le site « www.cartereduction-hertz.com » (identité, coordonnées, numéro de permis de conduire).

Prévenue le jour même par la CNIL, la société a alerté son sous-traitant en charge du développement du site, qui a immédiatement pris les mesures nécessaires permettant de mettre fin à l'incident. Au cours d'investigations complémentaires réalisées dans les locaux de la société et chez son sous-traitant, la CNIL a appris que la violation de données était la conséquence d'une suppression accidentelle d'une ligne de code avait entrainé le réaffichage des formulaires remplis par les adhérents.

La formation restreinte de la CNIL a prononcé le 18 juillet 2017 une sanction pécuniaire d'un montant de 40.000 euros, estimant que la société avait manqué à son obligation de prendre toutes les mesures pour préserver la sécurité des données personnelles des utilisateurs du site, conformément à l'article 34 de la loi Informatique et Libertés. Cette décision est la première rendue sous l'empire de la loi pour une République numérique qui prévoit une sanction pécuniaire maximum de 3.000.000 €.

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur les sinistres Cyber

DARTY

La Cnil a infligé en janvier 2018 une amende de 100 000 euros à Darty pour ne pas avoir suffisamment sécurisé les données de ses clients. En l'espèce, l'enseigne paie pour les erreurs de son sous-traitant, qu'elle aurait dû mieux contrôler en sa qualité de responsable du traitement. La décision de sévir contre Darty a été prise « en raison de la multitude de catégories de données traitées qui révèlent des informations sur les personnes et leur vie privée, au travers notamment des commandes passées », commente la formation restreinte, qui qualifie la situation de « grave ».

Cependant, Darty conserve la possibilité de faire appel cette décision devant le Conseil d'État. C'est d'ailleurs la perspective que l'entreprise suggère dans une réaction : « nous nous étonnons de cette décision et nous réservons nos droits au titre d'un éventuel recours », car la Cnil « n'a constaté aucune fuite de données » et que le prestataire a mis en œuvre, « à l'insu de Darty, une fonctionnalité de l'application que Darty n'avait pas sollicitée et n'a donc pas utilisée ».

La sanction rappelle en particulier que Darty endosse le rôle de responsable de traitement et qu'à ce titre, il lui appartient « de s'assurer et de vérifier que toutes les composantes et options de l'outil de gestion des demandes de service après-vente développées par [son sous-traitant] répondaient à l'obligation de confidentialité énoncée à l'article 34 de la loi précitée ».

Or, continue l'autorité, ses enquêteurs « ont pu accéder aux demandes de service après-vente formulées par les clients de la société, confirmant ainsi le défaut de sécurisation signalé par un tiers ». Dans la loi, « une violation de données est réalisée dès lors que des données à caractère personnel ont été rendues accessibles, volontairement ou non, à des tiers non autorisés », rappelle-t-elle.

CLEVER COURTAGE
IT Risk Insurance Broker

Retour d'expérience sur les sinistres Cyber

Pour résumer, la CNIL utilise les information fournie par des "lanceurs d'alerte" comme Zataz, dont on peut s'interroger sur la légitimité voire la licéité de l'action. A distance la CNIL réalise un contrôle en se fondant sur ces éléments et dresse procès-verbal, opposable au "délinquant".

Pour déclencher l'application de la garantie d'assurance :
- soit on se base sur la cause : défaut de sécurité au sens de l'article 34 de la loi informatique et libertés (idem dans le RGPD)
- soit on se base sur la conséquence : atteinte aux données à caractère personnel
- soit on se base sur le fait générateur « mise en cause » : la condamnation de la CNIL

Ou encore la combinaison des trois critères, défaut de sécurité ayant pour conséquence une atteinte aux données et ayant donné lieu à une condamnation de l'Autorité de Contrôle,

- Si la garantie d'assurance est déclenchée par le défaut de sécurité, il risque d'y avoir de beaux débats sur ce qu'est un défaut : défaut de conception, de programmation, de gestion sécuritaire, faille informatique,… !

- Si la garantie est déclenchée par l'atteinte aux données, alors dans le cas de Hertz et de Darty il n'y a pas eu atteinte effective aux données, ou rien ne permet de l'affirmer, il n'y a eu que constatation par les agents de la CNIL d'un défaut de programmation ou de fonctionnalité susceptible potentiellement de constituer un défaut de sécurité possiblement générateur d'une atteinte aux données, non avérées pour l'instant.

- Si la garantie est déclenchée par la condamnation de la CNIL, que se passe-t-il entre l'incident de sécurité et la condamnation de la CNIL pour accompagner l'assuré dans la gestion de crise ?

Claire Bernier
ADSTO
claire bernier@adsto.legal
+33 (0)6 73 80 26 37

Jean-Laurent SANTONI
Clever Courtage
jean-laurent.santoni@clevercourtage.com
+33 (0)6 25 79 13 28

Christophe DELCAMP
FFA
c.delcamp@ffa-assurance.fr
+33 (0)6 77 89 93 78