ANIA

Les Cyber Risques

13 avril 2015

Association Nationale des Industries Alimentaires

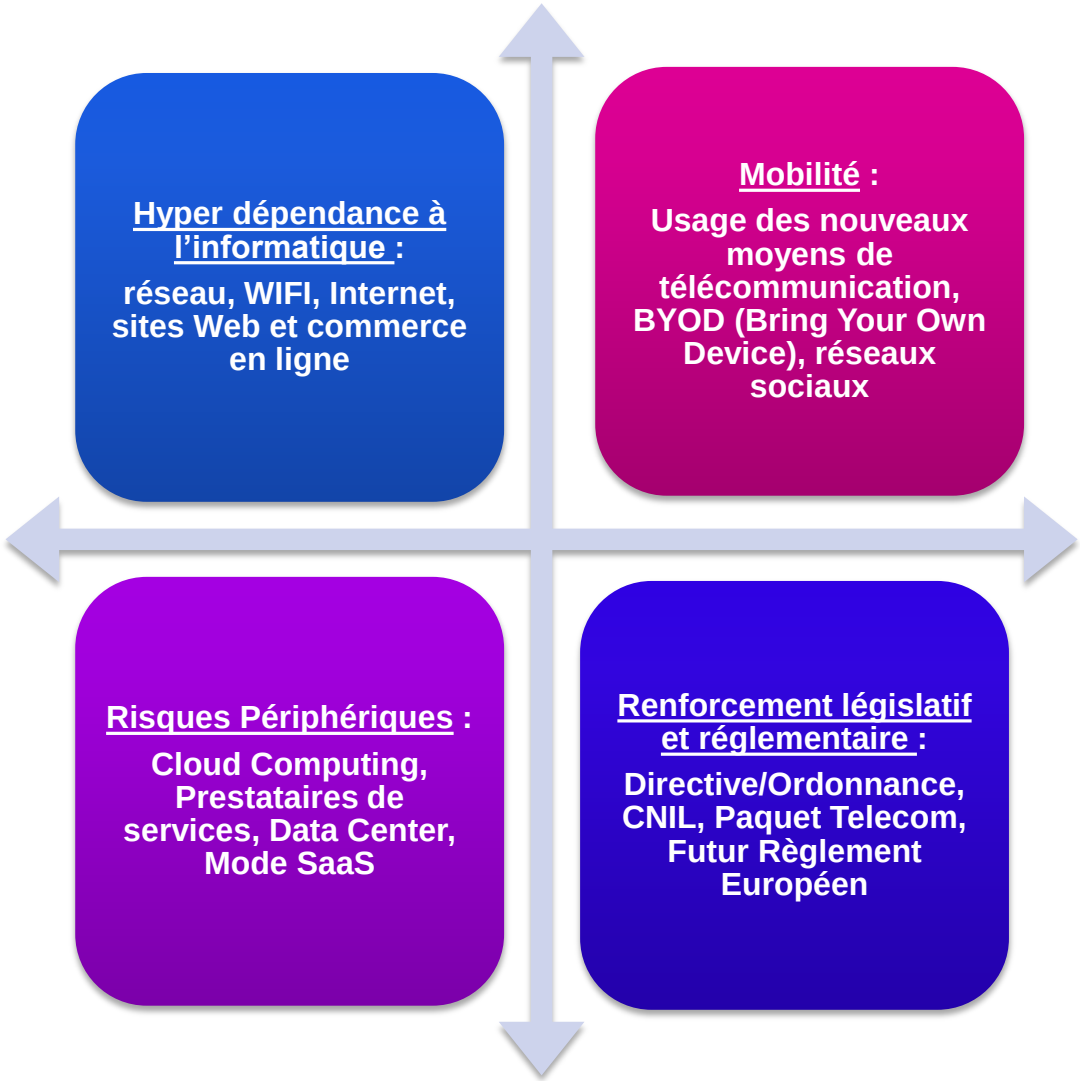
GRAS SAVOYE Willis
YOUR WORLDWIDE PARTNERS

Contexte

Les Principaux facteurs :

Aujourd'hui, envoyer un mail, créer des fichiers et les enregistrer dans un répertoire, surfer sur le net ou se connecter en wifi à un réseau public ou privé est devenu tellement usuel que nous n'y prêtons plus attention.

Etre protégé par un anti-virus et par un fire wall ne suffit plus. La question n'est pas de savoir si vous allez vous faire pirater, mais quand !

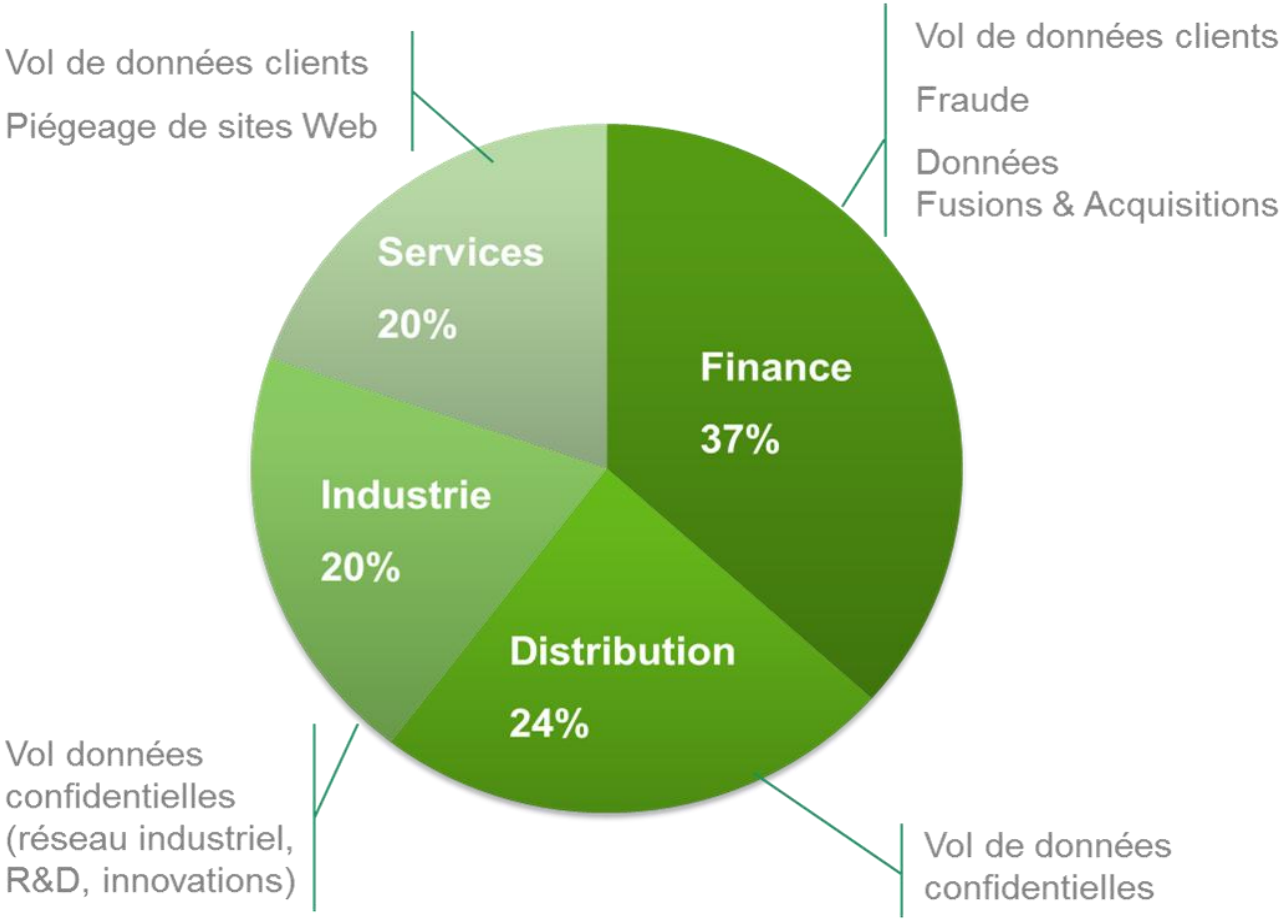


Aspects Législatifs et Règlementaires

	Depuis 1978 Loi Informatique et Libertés Cible : toute entreprise	Depuis 2011 « Paquet Telecom » Cible : FAI et prestataires télécom	Depuis 2013* Loi de Programmation Militaire Cible : OIV	Début 2016 Règlement Européen sur la protection des données Cible : Pout toute entreprise
Vos Obligations	Obligation de sécurité physique et logique du Système d'information	Obligation de sécurité du Système d'information (Obligation de moyen)	Obligation de résultat de notifier tous les incidents de sécurité à l'ANSSI	Obligation de Notification (Obligation de résultat) · À la CNIL, · Individuelle à chaque personne concernée
	Divulguer des informations par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 € d'amende	Obligation de Notification (Obligation de résultat) · À la CNIL, · Individuelle à chaque personne concernée.	Obligation de respecter des standards de sécurité (applicables aussi aux sous traitants)	Obligation de prendre toutes les mesures nécessaires pour remédier à l'incident.

* Décret d'application prévus fin 2014/ début 2015

Tous les secteurs sont touchés



Source : Rapport Verizon (2013)

La cybercriminalité en quelques chiffres

Des attaques réussissant très **rapidement**

84% des attaques réussissent en moins d'une journée

69% des exfiltrations ont lieu en moins d'une journée

Source : Verizon 2013

Des attaques auxquelles les grandes organisations **ne sont pas préparées**

243j en moyenne pour détecter une attaque ciblée

63% des attaques signalées par un tiers

Source : Mandiant 2013

Des **conséquences financières importantes**

1,7Mds€ de pertes engendrées en France

Source : ONDRP, 2010

2,5M€ perdus en moyenne par violation de données d'une entreprise en France

Source : Ponemon Institute, 2011

Qu'entend on par Cyber Risques?

Définition : les conséquences d'une atteinte aux données numériques détenues et/ou gérées par l'entreprise, que celles-ci lui appartiennent ou qu'elles lui soient confiées par des tiers, ainsi que les conséquences d'une atteinte au système informatique.

Les atteintes aux données numériques

- **Vos données** nécessaires à l'activité,
- **Les données appartenant aux Tiers**:
- Les données de vos collaborateurs,
- Les données des clients,
- Les données des fournisseurs, sociétés partenaires…
- **L'atteinte à la réputation**: diffamation, atteinte à la protection de la vie privée, atteinte aux droits à l'image, atteinte aux droits de propriété intellectuelle d'un tiers

Les atteintes au système informatique

- **Intrusion** dans les systèmes informatiques,
- **Interruption** des systèmes informatiques.
- **Contamination** des systèmes (virus, bombe logique…)
- **Utilisation illégale** des systèmes et du réseau.
- **L'atteinte à la réputation**: pertes de chiffre d'affaires, atteinte à l'image de la société…

Quelles sont les données à protéger et pourquoi?

Les données constituent un actif qu'il convient de protéger :

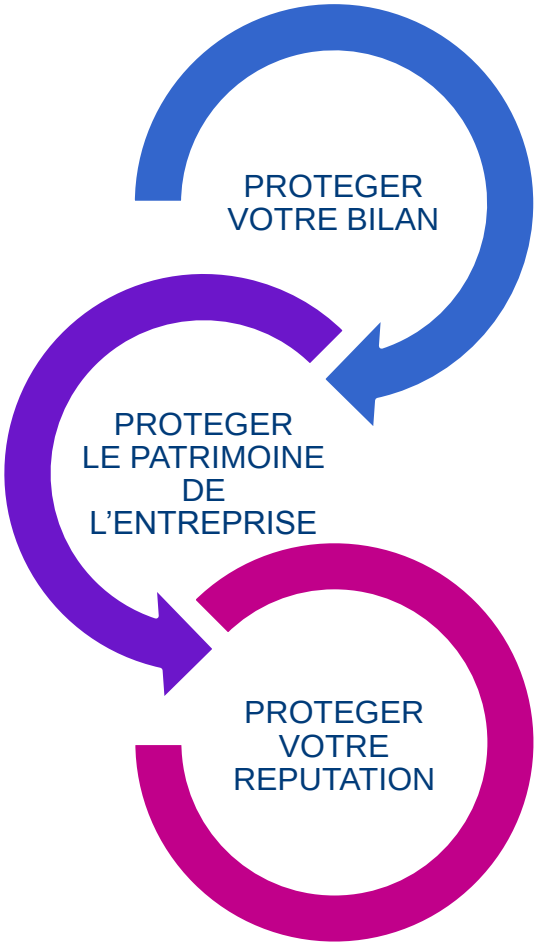
Données Personnelles :

Article 2 alinéa 2 de la Loi n° 78-17 du 6 janvier 1978 : « Constitue une donnée à caractère personnel, toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

Ex : nom, prénom, date de naissance, adresse postale, adresse électronique, adresse IP (d'un PC, mobile, imprimante), n° de téléphone, n° de carte de paiement, plaque d'immatriculation d'un véhicule, Adn, Photo, numéro de Sécurité Sociale ….

Données confidentielles:

Toute information, autre que des données personnelles, pour lesquelles l'Assuré est tenu à l 'égard d'un tiers au respect d'une obligation de confidentialité et qui sont conservées sur un système informatique détenu ou contrôlé par l'Assuré ou dont il est responsable.



Focus sur le risque de violation de la confidentialité des données personnelles

En France, Le coût moyen d'une violation des données s'élève à 127 € / données.
A titre d'exemple une violation impactant un fichier contenant 100.000 données clients, représente un coût de 12.700.000 €.

Les Garanties offertes par un contrat Cyber:

* La Garantie peut aussi relever de votre contrat Responsabilité Civile (à vérifier).

Typologie des risques

Atteinte aux données des tiers

Risque RC
(dans le cadre d'une réclamation de tiers)

- Vol et destruction des données
- Interruption des services en ligne et réclamations de tiers
- Corruption des données, ajout, transformation, cryptage, détérioration, altération
- Erreur
- Frais de Défense et Conséquences Pécuniaires

Atteinte aux données personnelles

Risques RC et Dommage
(avec ou sans réclamation de tiers)

- Frais de notification
- Frais de consultants (Forensics)
- Frais en cas d'enquête d'une autorité de contrôle
- Frais de Défense
- Sanctions Pécuniaires

Atteintes aux systèmes d'information ou aux données appartenant à l'assuré

Les Risques Dommages

- Vol, ajout, soustraction, détérioration, destruction
- Impossibilité d'utilisation des systèmes (Déni de service) / arrêt des systèmes
- Atteinte à l'image / gestion de crise / défaçage
- Contamination des systèmes et des données (attaque logique, virus…)
- Pertes d'Exploitation et les frais supplémentaires consécutifs

Les solutions d'assurance des Cyber-Risques

- **Ces sont des polices combinées offrant :**
  * des couvertures Dommages,
  * des couvertures Responsabilité Civile,
  * un volet assistance.

- **Ce sont des polices dédiées aux Cyber Risques, apportant une réponse unique à cette menace croissante**.

- **Ces contrats ont comme principaux avantages :**
  - prise en compte simple et rapide des garanties d'assurance en cas de cyber-attaques,
  - réactivité dans la gestion des sinistres (ex. : notification dans les délais impartis en cas de piratage des données personnelles).

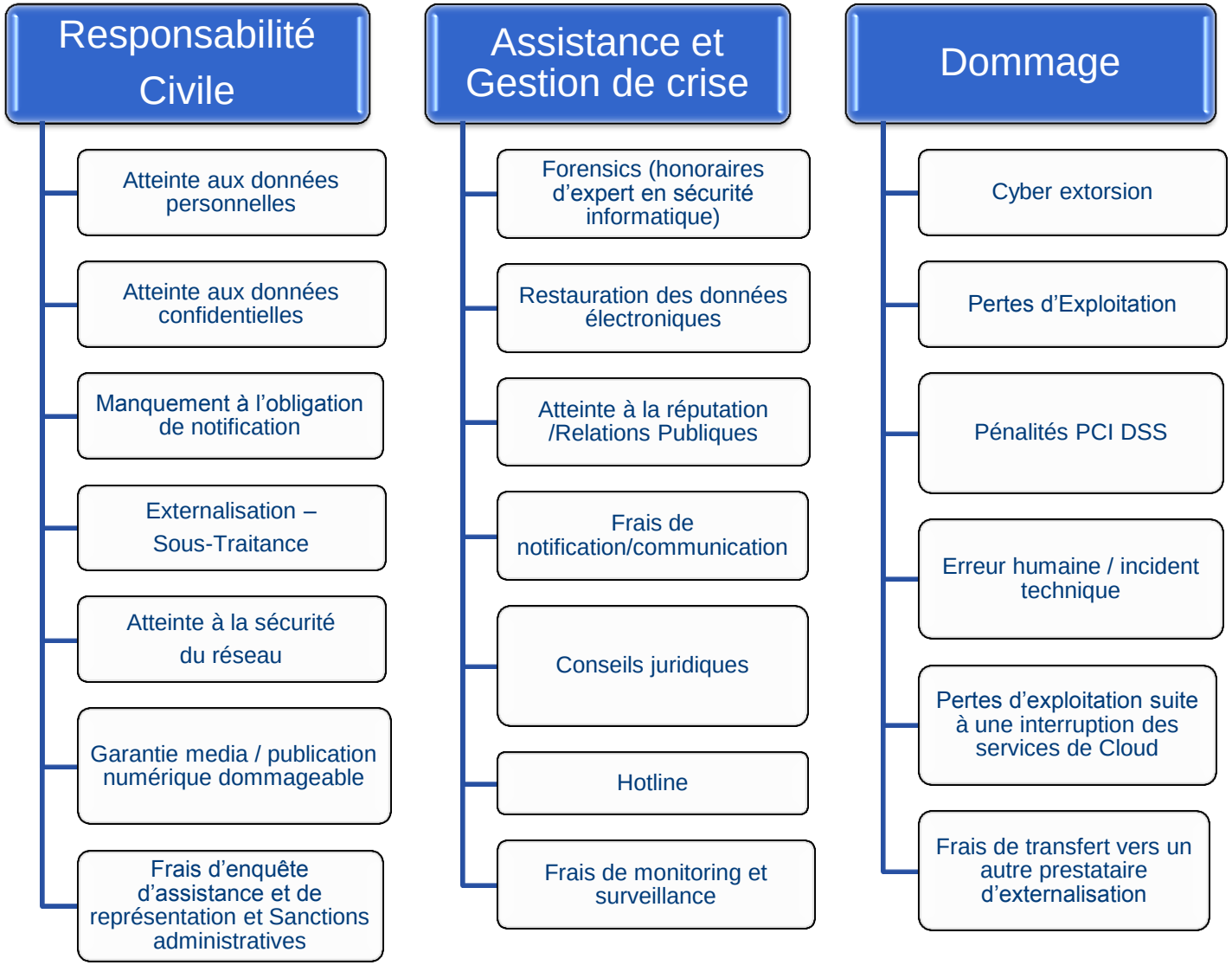
- **Ils peuvent intervenir en complément des garanties existantes dans les programmes d'assurances « traditionnels ».**

Il est important de noter que les garanties proposées au titre des polices Dommages et/ou Responsabilité Civile, sont :

- **généralement sous-limitées,**
- **partiellement couvertes.**

Enfin, des exclusions spécifiques peuvent restreindre le champ d'application des contrats.

Présentation des Garanties



Quelles garanties d'assurance suite à une atteinte?

	Type de Couvertures	suite à une atteinte au système d'information	suite à une atteinte aux données
Garanties Dommages	Frais de reconstitution des données		X
	Frais supplémentaires d'exploitation	X	X
	Pertes d'exploitation	X	
	Pénalités PCI-DSS		X
	Frais de gestion de crise/ Dépenses de Relations Publiques	X	X
	Extorsion de fonds (Cyber Extorsion)	X	X
	Frais de notification aux autorités administratives et aux Tiers		X
	Carence de Prestataires informatiques/ Infogérance	X	
	Frais de décontamination des systèmes d'information	X	
	Honoraires d'expert (Forensics, consultant informatique)	X	X
Garanties Responsabilité Civile	RC liée à la protection des données personnelles (Frais de Défenses et Conséquences Pécuniaires)		X
	RC liée à la sécurité des systèmes d'informations (Frais de Défenses et Conséquences Pécuniaires)	X	
	RC pour contenu d'un site internet/intranet (Diffamation, injures, calomnies, atteinte à la vie privée, à la propriété intellectuelle, divulgation d'informations confidentielles)		X
	Frais d'enquête, d'assistance et représentation devant des autorités administratives (CNIL/ANSSI pour les OIV)	X (si votre entreprise est un OIV)	X
	Sanctions Pécuniaires (ex : Amendes de la CNIL)	X	X
	Conséquences de la transmission de virus informatique subis par l'assuré	X	X

L'analyse des contrats traditionnels vs Cyber risques *

*** à vérifier au regard de vos contrats**

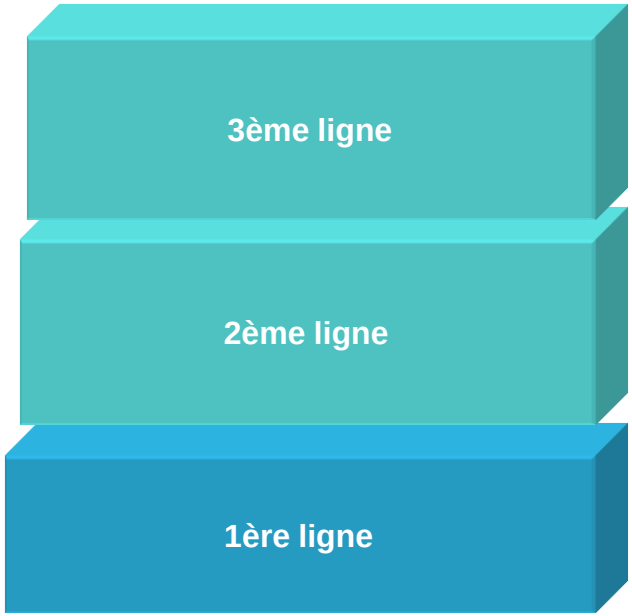
	Couvertures	Fraude	Risques Spéciaux	RCMS	RC Générale/RC Professionnelle	Dommages aux Biens / TRI	Contrat Cyber
Garanties Dommages	Frais de reconstitution des données						
	Frais supplémentaires d'exploitation					Si les données et les dommages immatériels sont couverts	
	Pertes d'exploitation						
	Pénalités PCI-DSS						
	Frais de gestion de crise/ Dépenses de Relations Publiques						
	Extorsion de fonds (Cyber Extorsion)		généralement sous limitée				
	Frais de notification aux autorités administratives et aux Tiers						
	Carence de Prestataires informatiques/ Infogérance						
	Frais de décontamination des systèmes d'information						
	Honoraires d'expert (Forensics, consultant informatique)						
Garanties RC	RC liée à la protection des données personnelles (Frais de Défenses et Conséquences Pécuniaires)						
	RC liée à la sécurité des systèmes d'informations (Frais de Défenses et Conséquences Pécuniaires)						
	RC pour contenu d'un site internet/intranet (Diffamation, injures, calomnies, atteinte à la vie privée, à la propriété intellectuelle, divulgation d'informations confidentielles)						
	Frais d'enquête, d'assistance et représentation devant des autorités administratives (CNIL)						
	Sanctions Pécuniaires (ex : Amendes de la CNIL)						
	Conséquences de la transmission de virus informatique subis par l'assuré						

	la garantie peut exister
	la garantie existe généralement
	la garantie n'existe pas/ est exclue / ce n'est pas l'objet du contrat

Les différentes options de mise en place d'une Police Cyber risques

Police/Programme Cyber

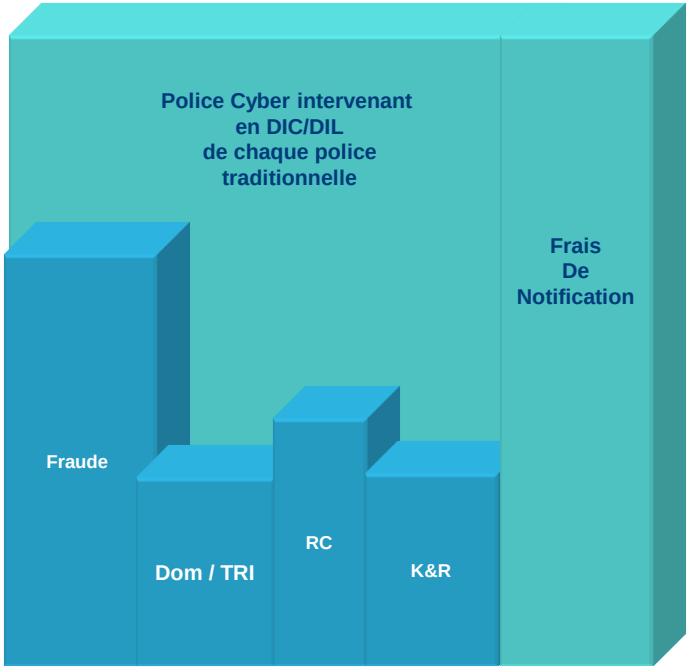
Police Cyber Stand Alone



Avantages :
Une police unique et dédiée aux risques Cyber,
Une confidentialité assurée,
Un sinistre déclaré et instruit auprès d'un seul interlocuteur.
Les polices traditionnelles peuvent intervenir en complément, le cas échéant,

Inconvénients:
Quelques garanties ça et là en doublon de celles existantes dans les contrats dits traditionnels.

en DIC/DIL



Avantages :
Un achat uniquement pour un sinistre d'intensité
Un relatif avantage budgétaire

Inconvénients :
Divulgation des polices sous jacentes (problème de confidentialité),
Plusieurs assureurs et leurs experts respectifs vont gérer un seul et même sinistre,
Un sinistre Cyber peut grever vos statistiques et épuiser des garanties qui n'ont initialement pas été souscrites pour ce type de risque,

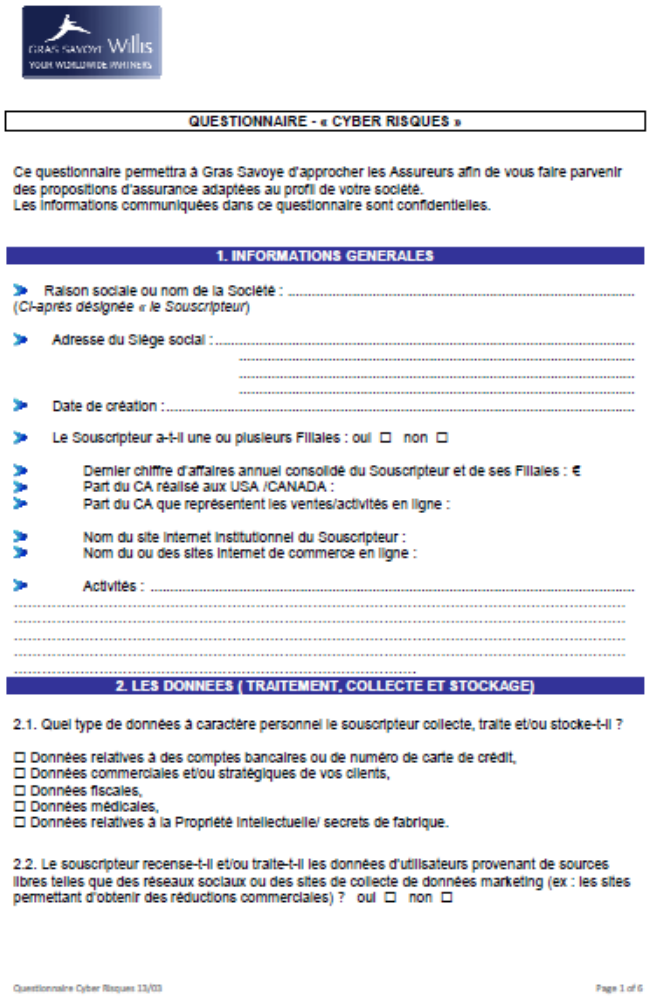
Le marché de l'assurance - acteurs et capacité

Assureur	Capacité théorique	Rating S&P
ACE	De 20M€ à 50 M€	AA - stable
AGCS	50 M€ à 100M€	AA négatif
AIG	25 M€ + 100M€ en excess	A stable
AXA CS	25M€	A + stable
Beazley	25 M€	A + fort
Chubb	10 M€	AA stable
CNA	10 M€	A fort
Hiscox	15 M€	A stable
Munich Re CIP	150 M€	AA - stable
QBE	10 M€	A + négatif
SRI (Swiss Re International)	25 M€	AA - stable
XL	15 M€	A stable
ZURICH	25 M€	AA - stable
Total marché français	De 405 M€ à 570 M€	

En complément des capacités théoriques du marché français, nous faisons appel au

- marché de Londres avec plus de 100M€ supplémentaires,
- marché US avec 1,5milliard de $.

L'Offre Gras Savoye :



QUESTIONNAIRE - « CYBER RISQUES »

Ce questionnaire permettra à Gras Savoye d'approcher les Assureurs afin de vous faire parvenir des propositions d'assurance adaptées au profil de votre société.
Les informations communiquées dans ce questionnaire sont confidentielles.

1. INFORMATIONS GENERALES

- Raison sociale ou nom de la Société : .....
(*Ci-après désignée « le Souscripteur*)
- Adresse du Siège social : .....
.....
.....
.....
- Date de création : .....
- Le Souscripteur a-t-il une ou plusieurs Filiales : oui ☐ non ☐
- Dernier chiffre d'affaires annuel consolidé du Souscripteur et de ses Filiales : €
- Part du CA réalisé aux USA /CANADA :
- Part du CA que représentent les ventes/activités en ligne :
- Nom du site Internet institutionnel du Souscripteur :
- Nom du ou des sites Internet de commerce en ligne :
- Activités : .....
.....
.....
.....
.....
.....

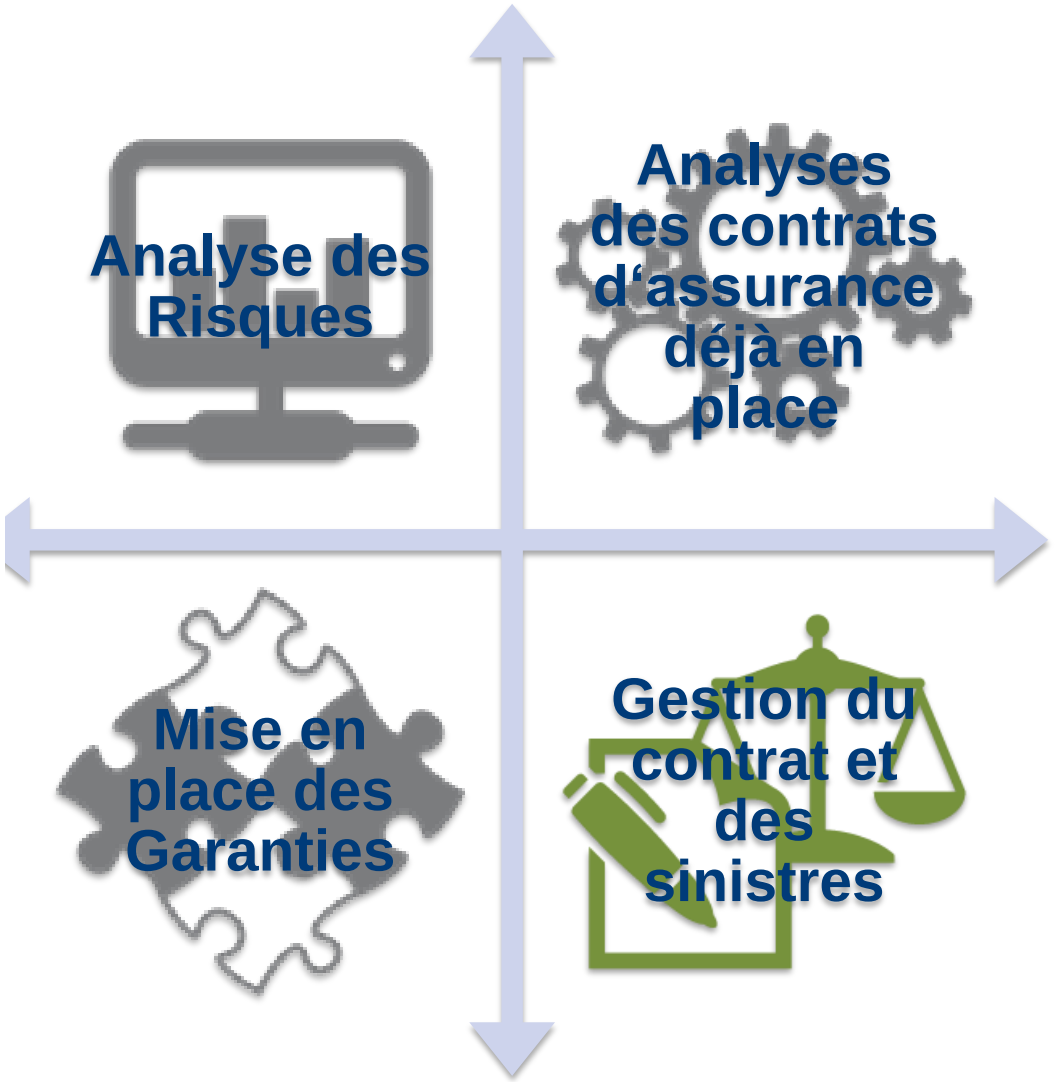
2. LES DONNEES (TRAITEMENT, COLLECTE ET STOCKAGE)

2.1. Quel type de données à caractère personnel le souscripteur collecte, traite et/ou stocke-t-il ?

☐ Données relatives à des comptes bancaires ou de numéro de carte de crédit,
☐ Données commerciales et/ou stratégiques de vos clients,
☐ Données fiscales,
☐ Données médicales,
☐ Données relatives à la Propriété Intellectuelle/ secrets de fabrique.

2.2. Le souscripteur recense-t-il et/ou traite-t-il les données d'utilisateurs provenant de sources libres telles que des réseaux sociaux ou des sites de collecte de données marketing (ex : les sites permettant d'obtenir des réductions commerciales) ? oui ☐ non ☐

Questionnaire Cyber Risques 13/03 Page 1 of 6



Contacts

- **Laure ZICRY**
- Responsable Technique Institutions Financières et Practice Leader Cyber Risks
- Gras Savoye Corporate Risk Management
- FINEX Lignes Financières

- Direct : + 33 (0) 1 41 43 51 82
- Mobile : + 33 (0) 6 68 98 52 84
- **laure.zicry@grassavoye.com**