



Le rendez-vous des entreprises qui innovent



LE COURTIER DES SOCIÉTÉS INNOVANTES

L'Assurance des Cyber Risques Systèmes Embarqués

1. Les fondamentaux
2. Cyber risques

1. Rappel des fondamentaux



Assurance de responsabilité civile « RC »

- L'objet est de garantir les conséquences pécuniaires de la responsabilité civile pouvant incomber à l'assuré en cas de dommages causés aux tiers
- Conditions : une réclamation d'un tiers ; un risque de préjudice du tiers ; et une mise en jeu de la responsabilité de l'assuré
- L'indemnité d'assurance :
 - Le préjudice → pour le tiers**
 - Les frais de défense → pour l'assuré**

Assurance de dommage aux biens – pertes financières

- L'objet est de garantir l'assuré contre les risques de perte ou de dégradation de ses biens ou biens confiés et leurs conséquences financières (frais supplémentaires, PE)
- L'indemnité d'assurance :
 - Les frais, la valeur du bien et la perte de marge brute d'exploitation → pour l'assuré**

1. Rappel des fondamentaux



Dommmage

- C'est une perte pécuniaire ou une atteinte à un droit

Préjudice

- Le préjudice est le dommage qui est causé à autrui d'une manière volontaire ou involontaire

Commentaires

- La différence entre le dommage et la préjudice est liée à l'imputabilité
- Les contrats de RC excluent les dommages qui portent sur les factures, le coût de la prestation de l'assuré et les redevances des licences

1. Rappel des fondamentaux



Dommmage corporel

- Atteinte à l'intégrité physique d'une personne

Dommmage matériel

- Atteinte à un bien tangible

Dommmage immatériel

- Ce qui n'est pas un dommmage corporel ou matériel
- Donc, frais et pertes financières (manque à gagner, perte de CA, surcoûts etc.)

Dommmage immatériel consécutif

- Un dommmage immatériel (pertes financières) consécutif à un dommmage corporel ou matériel

Dommmage immatériel non consécutif

- Un dommmage immatériel non consécutif à un dommmage corporel ou matériel

- Pas de définition légale
- De nombreuses définitions possibles hétérogènes et avec des périmètres différents
- Définitions proposées :
 - **« Les risques liés à l'utilisation de SI connecté à un réseau ouvert »**
 - **« Conséquences des atteintes aux données et aux SI »**
 - pour l'assuré : ses données, son SI
 - pour le tiers ; son préjudice

3. Cyber Risques - Approche par les Sources

APPROCHE PAR LES SOURCES

SPHÈRE CYBER

■ Les cyber maffias

Elles sont uniquement motivées par l'argent qu'elles peuvent extorquer à l'assuré (i) en le faisant chanter (ii), en lui volant les données de son SI pour les revendre (iii), ou bien elles utilisent le SI de l'assuré pour nuire à d'autres victimes (attaque par déni de service par exemple).

■ Les hackers

Ils cherchent la notoriété (plus un SI est réputé sécurisé et plus il constituera une prise de valeur pour un Hacker ; y penser dans la communication...) ; ils veulent aussi se mesurer aux meilleures sécurités pour acquérir de nouvelles connaissances.

SPHÈRE ÉCONOMIQUE

■ Les acteurs de l'intelligence économique « noire »

Les concurrents de l'assuré (plutôt leurs agents) qui essaient de se procurer illégalement (critère de l'information « noire » par rapport à la « blanche » et même la « grise ») des informations sur sa stratégie pour mieux ajuster la leur : ils cherchent des mails, des mémos de réunion, etc... Les plus malhonnêtes peuvent envisager de voler les secrets industriels de l'assuré pour les réutiliser à leur profit ; voire, saboter son outil de production pour le retarder.

■ Les États

Douanes, Fisc, autorités de la concurrence... Certains Etats n'ont pas hésité à utiliser les données piratées dans les SI des banques suisses...

SPHÈRE POLITIQUE

■ Les terroristes

Ils cherchent à commettre des cyber-attentats ; en outre, ils utilisent des données volées dans les SI pour aider à la préparation de leurs attentats dans le monde « réel ».

■ Des hacktivistes

« Le hacktivism est une contraction de hacker et activisme. Ici se trouvent simultanément les savoir-faire technologiques et analyses politiques [...] » (Wikipédia) ; ils cherchent à médiatiser leur cause et/ou à nuire à l'assuré s'ils estiment que son activité heurte leur philosophie : entreprises militaires, agroalimentaires, polluantes, etc.

✓ Il est important de déterminer l'origine des menaces, car certaines origines font l'objet d'exclusions de la part des assureurs : par exemple, les terroristes et dans une certaine mesure, par extension, les activistes.

APPROCHE PAR LES MENACES : **CAUSES TECHNIQUES**

MENACES VIA LE SI DE L'ASSURÉ

- Malwares
- Intrusion
- Mauvaise utilisation du SI

MENACES VIA D'AUTRES SI

- Attaque type déni de service
- Hameçonnage
- Cybersquatting
- Atteinte à l'e-réputation

MENACES : AUTRES

- Ingénierie sociale

2. Cyber Risques - Cartographie

CARTOGRAPHIE DES CYBER RISQUES



LE COURTIER DES SOCIÉTÉS INNOVANTES

1 - SOURCES DES MENACES

SPHÈRE CYBER

- Cyber Maffias
- Hackers

SPHÈRE ÉCONOMIQUE

- Concurrents
- Acteurs de «l'Intelligence Économique
- États

SPHÈRE POLITIQUE

- Hactivistes
- Terroristes
- États

2 - CAUSES TECHNIQUES

MENACES VIA LE SI DE L'ASSURÉ

- Malwares
- Intrusion
- Mauvaise utilisation du SI

MENACES VIA D'AUTRES SI

- Attaque type déni de service
- Hameçonnage
- Cybersquatting
- Atteinte à l'e-réputation

MENACES : AUTRES

- Ingénierie sociale

3 - CONSÉQUENCES OPÉRATIONNELLES

LARGEMENT COUVERT

- Perte/destruction de données de l'assuré ou de données tierces sous sa garde
- Divulgaration de données personnelles ou confidentielles
- Violation par l'assuré de ses obligations légales ou contractuelles quant à la sécurité des données et la protection des données personnelles
- Nécessité d'identifier la faille de sécurité, d'y remédier, de reconstituer les données, de notifier pour les données personnelles, de communiquer, éventuellement d'activer un PCA, ...

EXCLUSIONS IMPORTANTES

- Déni de service du SI de l'assuré
- Utilisation des ressources du SI de l'assuré / pertes de performance
- Conséquences des contrefaçons, délits de presse, etc. commis via le site web de l'assuré
- Conséquences des cyber-délits commis via le SI de l'assuré : attaque déni de service, spam, etc.

EXCLUSIONS CRITIQUES

- Atteintes aux logiciels/traitements du SI de l'assuré
- Comportement aberrant du SI de l'assuré ou d'un SI tiers suite à une altération des traitements ou des données non détectée par l'assuré
- Conséquences de tous les délits commis via le SI de l'assuré (hors site internet et cyber-délits)
- Non respect par l'assuré de ses engagements contractuels de service (SLA en particulier)

NON GARANTI

- Vol de données entraînant une perte de valeur des données (plans, codes informatiques, contenu)
- Atteintes aux logiciels / traitements d'un SI via le SI de l'assuré
- Dommages matériels et corporels commis via le SI

4 - ASSURANCE DES MENACES

- Dommage, frais, PE, RC, ...
- Pour l'assuré et pour les tiers
- Voir plus loin les contrats d'assurance «Cyber» déjà sur le marché

Liste des risques à assurer, donc à financer !

■ 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 à la propriété intellectuelle ou d'une atteinte à la vie privée ou du droit à l'image
- ❑ Conséquences d'agissement diffamatoire, de publicité mensongère ou de dénigrement
- ❑ Conséquences d'une atteinte du SI ou des données d'un tiers via le SI de l'assuré
- ❑ Conséquences d'un déni de service suite à une attaque logique
- ❑ Conséquences d'une transmission de virus à d'autres

■ Volet Gestion de crise

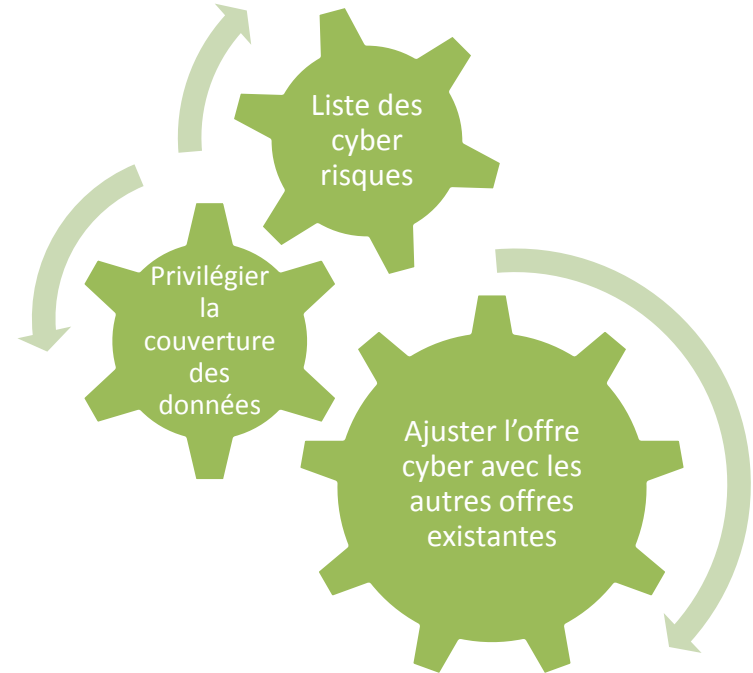
- ❑ Frais pour l'indentification des causes
- ❑ Frais de représentation suite à une convocation ou enquête de la CNIL
- ❑ Frais de notification suite à une injonction de la CNIL
- ❑ Frais de notification suite une obligation contractuelle
- ❑ Frais de monitoring
- ❑ Frais de communication
- ❑ Frais de consultant en sécurité informatique
- ❑ Frais de consultant en cas de tentative d'extorsion (K&R)

■ Volet DB

- ❑ Frais de reconstitution des données et frais de restauration des sauvegardes suite à une atteinte aux données et aux SI
- ❑ Frais de recherche et frais de décontamination suite à une atteinte aux données et aux SI
- ❑ Frais supplémentaires d'exploitation, PE suite à une atteinte aux données et aux SI
- ❑ Pénalité contractuelle ou SLA suite à une atteinte aux données ou aux SI
- ❑ Conséquences pécuniaires suite à un déni de service
- ❑ Frais de mise en œuvre du PCA

■ Conception

Selon nous, aucun des contrats analysés n'a été conçu à partir d'une définition théorique des Cyber-Risques ; l'architecture de ces contrats ressemble plutôt à un inventaire de risques ordonnés selon trois axes :



2. Cyber Risques - Approche des assureurs actuels



- Conception Certains contrats abordent le sujet avec une démarche pragmatique utile aux PME : ils proposent des services avec une assistance en sus des garanties (par exemple cellule de gestion de crise, « identity monitoring », hotline, etc.) en cas de difficulté ; d'autres contrats sont d'inspiration plus classique
- Les différents contrats du marché sont donc assez différents...
- Tous les contrats présentent des lacunes (i) soit par volonté des assureurs de ne pas assurer certains risques (ii) soit aussi parce que beaucoup de Cyber-Risques sont inassurables pour des raisons techniques et/ou juridiques (la question de l'assurance des conséquences des infractions non-intentionnelles irrigue toute la problématique)
- Enfin, l'émergence du Cloud Computing semble insuffisamment prise en compte...

- **Cyber risques déjà couverts dans les programmes RC et de Dommages aux biens (DB)**
 - Pas d'exclusion en RC et en DB
 - Couvertures des conséquences des attaques logiques pour les pertes financières en DB
 - Couvertures des dommages indirectes sans dommages directes en DB
- **Adaptation des polices (RC et DB) du programme de Syntec numérique**
 - Ajout d'un volet gestion de crise et frais de prévention

2. Cyber risques - Traitement des Cyber Risques pour SNA (2/2)



- **Pourquoi une police spécifique :**
 - Pour répondre à des demandes spécifiques
 - Pour répondre à des besoins de capacité
- **Lancement d'une police spécifique Cyber Syntec en 2016**
 - Texte courtier rédigé pour le SNA : unique sur le marché de l'assurance
 - Une rédaction simplifiée :
 - Une meilleure compréhension
 - Mieux de suivre les évolutions sans trop de changement
 - Très peu de sous limitation
 - Facilité de souscription avec un questionnaire réduit au stricte minimum
 - Tarifs négociés



LE COURTIER DES SOCIÉTÉS INNOVANTES

Nicolas Hélénou | Co-gérant (nhelenon@lsngroupe.com)

Benoît Lemaire | Co-gérant (blemaire@lsngroupe.com)

Colin Crombac | Consultant (ccrombac@lsngroupe.com)

Paul-Louis Heslout | Chargée de clientèle (plheslout@lsngroupe.com)