ASSOCIATION
EUROPE
FINANCES
RÉGULATIONS

Matinale sur l'assurabilité des risques cyber

25 mars 2022

Patrick DEGIOVANNI – Directeur Général Adjoint de Pacifica

Chapitre 1
RISQUE CYBER, DE QUOI PARLONS-NOUS ?

Les cyber risques, qu'est-ce que c'est ?

Une cyber attaque est un **acte malveillant envers un dispositif informatique**, qui peut émaner d'une personne seule, comme d'une organisation très structurée. Les **atteintes** portent sur les **données** et les **systèmes d'information.**

Selon la « règle des 6 i », une cyber attaque peut être :
invisible, intensive, incompréhensible, internationale, incertaine, intentionnelle.

Elle peut provenir:

De l'intérieur : Employés, voleurs, erreurs d'inattention…

De l'extérieur : Bandes organisées, hackers, amateurs…

LES PRINCIPALES CYBER ATTAQUES

« Ransowmare » :
blocage des données et demande de rançon

« Phishing » :
vol des données personnelles

« Malware » :
propagation d'un virus, cheval de troie

« Wiper » :
Détruit les données infectées

Vol des données

Atteinte à l'e-réputation

Entrave à l'activité

Coût financier important

Quelques chiffres

LE RISQUE CYBER
EN FRANCE ET DANS LE MONDE

6 000 Md$
C'est le coût de la cybercriminalité au niveau mondial attendu pour 2021, tous secteurs confondus, **contre 3 000 milliards de $ en 2015**

3ème
C'est la place qu'occuperait le cyberrisque dans l'économie mondial **s'il était un pays**

43%
C'est le pourcentage de PME qui ont constaté **un incident de cybersécurité** en 2020

16%
C'est le pourcentage des cyberattaques qui **menacent la survie** d'une entreprise en 2020

x4
C'est **l'augmentation des attaques** au rançongiciel entre 2020 et 2021, selon l'ANSSI

6/10
6 PME sur 10 font **faillite dans les 6 mois** après une cyber-attaque

Données provenant du rapport CEA octobre 2021
Données provenant du rapport FFA du 29 juin 2021

LE MARCHÉ DE LA CYBER-ASSURANCE
EN 2020 EN FRANCE

Le développement de la cyber-assurance a fait face à deux freins ces dernières années :
- **La difficulté à modéliser les risques cyber** (peu d'historique, la probabilité de subir une attaque et son ampleur évolue avec les technologies etc.) qui rend les contrats onéreux
- **La propension faible des entreprises à payer pour ce type de couverture** (manque de connaissance des risques encourus, peu de communication sur les cyber-attaques etc.).

France Assureurs

135 M€ Estimation des cotisations 2020 dont 90% provenant de contrats Cyber dédiés => ***+29% par rapport à 2019***

68% S/C Soit 84 millions d'€ en 2020 ***+190% par rapport à 2019***

Entreprises françaises assurées en France

AMRAE

130 M€ **+ 49,4% par rapport à 2019**

167% S/C Soit 217 millions d'€ en 2020 / ***+ 194% par rapport à 2019***

Entreprises françaises et ses filiales européennes assurées en France

TAUX DE COUVERTURE DES ENTREPRISES EN ASSURANCE CYBER (DONNÉES AMRAE) :

87%
GRANDES ENTREPRISES
+22,2% par rapport à 2019

8%
ETI
+43,6% par rapport à 2019

0,0026%
PME
+16,3% par rapport à 2019

La structuration de l'offre Cyber sur le marché

Une répartition de l'offre Cyber actuellement proposée sur le marché s'observe sur la base de 3 piliers principaux :

Diagnostic de l'existant

Plusieurs acteurs de place proposent une phase de diagnostic du **niveau de vulnérabilité du système** en place chez le prospect/client.

3 types de diagnostic peuvent être réalisés :

- → Auto-diagnostic sur le site internet de l'acteur
- → Audit Cyber sécurité
- → Audit technique (incluant une mise en situation d'attaque Cyber)

Traitement à froid des axes d'amélioration identifiés

Après avoir identifiés certaines anomalies dans le système mis en place par le client, certains acteurs de place proposent des solutions clés en main afin de les traiter:

- → Mise à disposition d'outils
- → Certifications
- → Amélioration des process
- → Sécurisation des données
- → Formation des collaborateurs

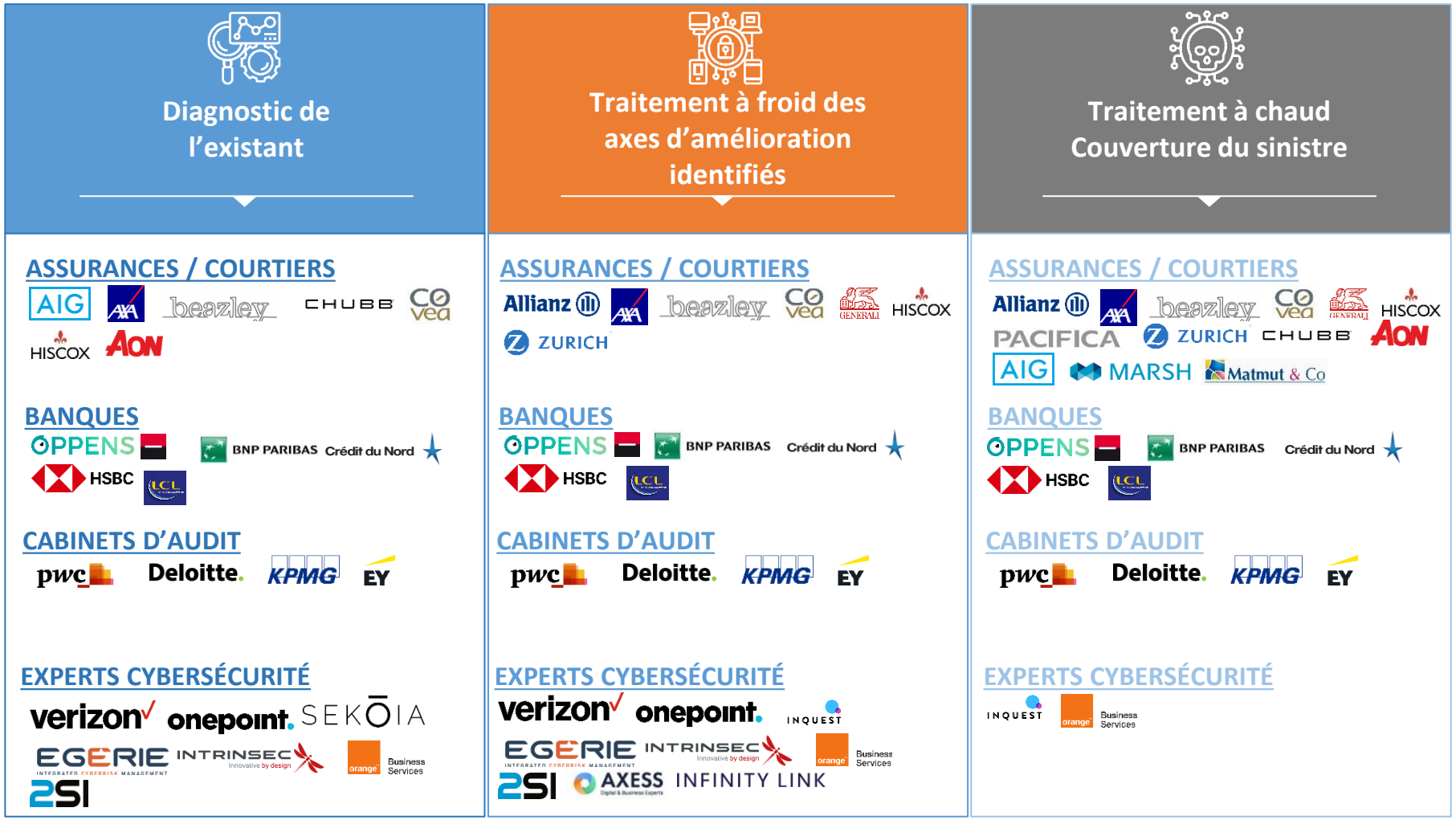
Traitement à chaud Couverture du sinistre

Pilier privilégié du secteur assurantiel, la couverture du sinistre s'analyse principalement par :

- → La **mise à disposition d'experts**
- → La **couverture des frais engendrés** par le sinistre (reconstitution des données, matériel endommagé etc.)
- → La couverture des **frais juridiques** (incluant frais de notification)

Un marché qui se structure de plus en plus autour de cette proposition de valeur

Etat des lieux du marché de l'offre Cyber (vision fin 2021)



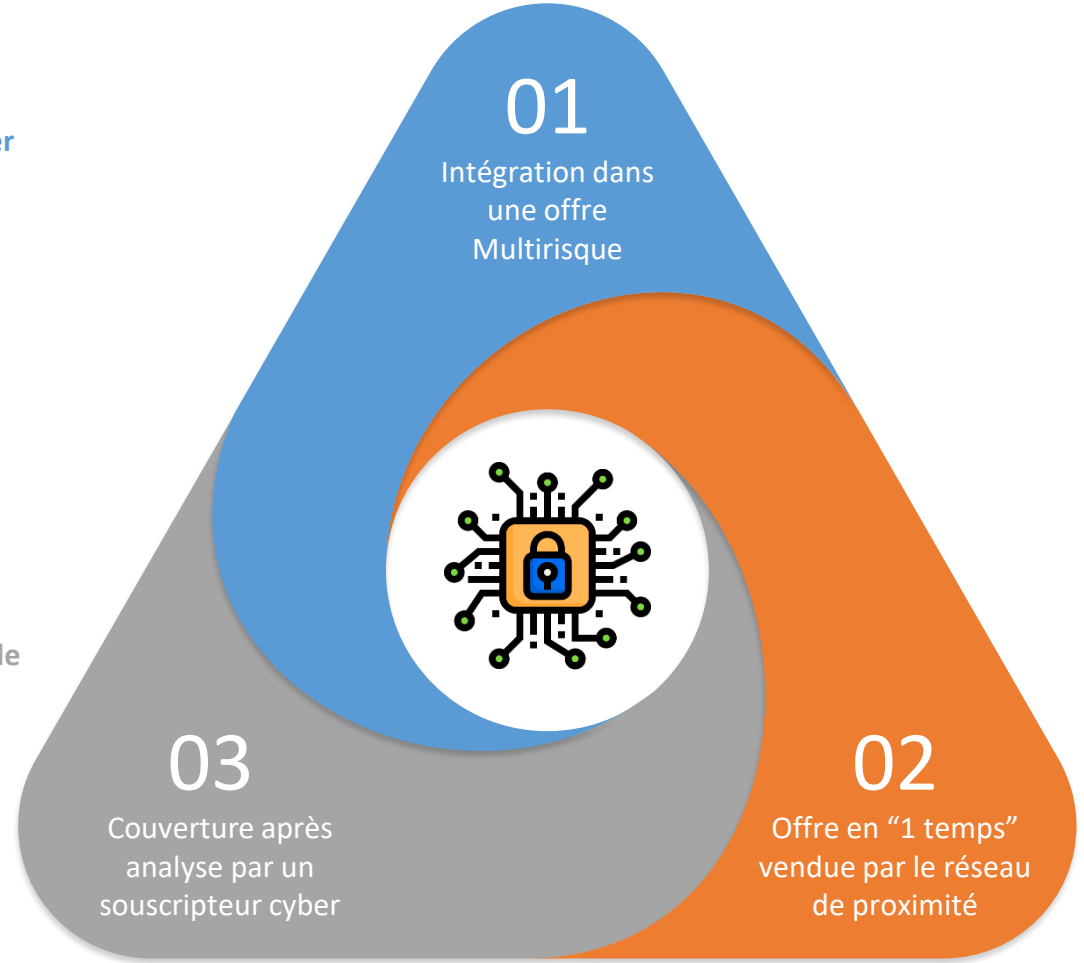
Un positionnement des assureurs selon 3 axes

Automatisé

01 **Certains assureurs incluent au sein de leur offre Multirisque une couverture cyber avec un plafond limité pour le risque cyber de ses clients (quelques dizaines de milliers d'euros)**

02 **Les assureurs proposent également une offre dédiée à la couverture du risque cyber des entreprises vendue en « sec »**

03 **Sur la clientèle PME-ETI et Grandes Entreprises, l'assurance est souscrite après analyse par un souscripteur cyber qui sur la base d'un questionnaire complet (plusieurs pages), et d'échanges complémentaires avec le client, accepte ou non le risque, affine le tarif et les conditions du contrat d'assurances.**



Chapitre 2
LE RISQUE CYBER AU CŒUR DE L'ACTUALITÉ

Un risque cyber au cœur de l'actualité

La sinistralité

- Depuis 2020, la sinistralité s'intensifie chez l'ensemble des assureurs, à la fois en fréquence (nombre de sinistres) et sévérité (montant / sinistre)
- De nombreux assureurs subissent une forte dégradation de leur ratio combiné et entendent redresser leur portefeuille

→ Effet sur la capacité : les assureurs réduisent leurs engagements
→ Effet sur les garanties : certains risques (ex : ransomware) ne sont plus couverts ou restreints, les questionnaires sont plus exigeants
→ Les primes augmentent : entre x2 et x4 observés sur le marché

La réglementation

- L'assurance de certaines garanties propres aux polices cyber fait débat : les garanties « indemnisation de la rançon » et « prise en charge des sanctions en cas d'atteinte à la confidentialité des données personnelles » sont regardées à la loupe
- Le législateur encadrera probablement ces garanties (Cf. slides suivants)

→ Une clarification du sujet est en cours sur le paiement de la rançon
→ Certains assureurs se sont positionnés et ne couvrent plus le paiement de la rançon en attendant que ce flou juridique soit levé

Les cumuls d'engagements

- Les assureurs redoutent les garanties silencieuses (garanties de polices dommages qui n'excluent pas le fait générateur d'origine Cyber) qui viendraient en cumul des garanties d'une police cyber
- Les polices cyber sont précisées afin d'exclure certains risques garantis par d'autres polices (RC Professionnelle, Fraude, Dommages)

→ Dans les meilleurs cas, les exclusions déjà prévues sont précisées, dans les pires les garanties sont restreintes

L'assurabilité du risque Cyber en question

- Le caractère potentiellement systémique à l'échelle d'un territoire suscite à juste titre l'inquiétude des assureurs
- Les pressions exercées sur le marché de l'assurance conduisent des entreprises à revoir leur politique d'assurance de ce risque (internalisation par les grands groupes)

→ Les assureurs pourraient souffrir d'une faible mutualisation, voire d'une mauvaise diversification du risque
→ La question du soutien par l'état en cas de « pandémie » reste entière

Point de vue des différentes parties prenantes

France Assureurs / Assureurs

Demande de clarification du sujet afin que les assureurs puissent se positionner quant à la légalité de la cyber-rançon.

AXA s'est désengagé du paiement de la rançon il y a quelques mois (après l'avoir ajoutée).
Generali vient de retirer cette garantie sur son offre à destination des grandes entreprises.

HCJP

« Dès lors que les dispositifs français et internationaux visant à lutter contre le terrorisme et le crime organisé sont respectés, compte tenu du besoin des victimes de se garantir contre le risque de ransomware et du marché européen dans lequel évoluent les entreprises d'assurance, interdire l'assurabilité du remboursement des rançons en cas de cyber attaque par un texte législatif national, n'est pas préconisé

MAIS certains axes d'amélioration sont proposés :

Ordre opérationnel : proposer d'imposer et faciliter les dépôts de plaintes par les victimes
Ordre réglementaire : élaborer au niveau national un cadre clair et disponible à tous : Mise en place d'une autorité unique comme proposée aux Etats-Unis, dotée de pouvoirs suffisants pour mettre en place un site internet qui pourrait assister les victimes et permettre un échange d'information.
Prévention : agir pour que les entreprises ne communiquent pas dans leurs rapports annuels des informations sur la protection contre le risque cyber et faire en sorte que les appels d'offre des organismes publics soient confidentiels et les demandes de couverture contre les risques cyber n'apparaissent pas. »

Ministère des finances

« Rançons : Obligation (ou incitation via accord de place) de dépôt de plainte, amélioration de la coordination entre autorités publiques compétentes (voir dispositifs d'alertes de la part des assureurs), mesures de prévention »

Point de vue des différentes parties prenantes

Rapport parlementaire Cyber-assurance

« Pour toutes ces raisons, il convient d'inscrire dans la loi l'interdiction pour les assureurs de garantir, couvrir ou d'indemniser la rançon et se porter davantage vers la prévention, l'accompagnement et l'assurance des conséquences pour une entreprise.

De même à l'instar de nos collègues américains, il convient de sanctionner les entreprises, administrations ou collectivités qui procèdent au paiement des rançons à l'aide d'un tiers ou de manière direct. »
Page 13-14 du rapport

ANSSI

Selon Guillaume Poupard (DG ANSSI) : Les assureurs « préfèrent payer quelques millions de rançons plutôt que quelques dizaines de millions au titre de la perte des données garantie par la police d'assurance contractée. Nous devons mener un travail de fond pour casser ce cercle vicieux autour du paiement des rançons. »

L'ANSSI est contre le paiement de la rançon par les assureurs car celle-ci permet le financement d'un éco-système criminel

En conclusion :

Un projet de loi est en cours afin de faire inscrire dans le Code des Assurances (article L. 12-10-1 du Code des assurances) l'obligation d'un dépôt de plainte par la victime dans les 48h après le paiement de la rançon rendant cette prestation légale et assurable.

Chapitre 3
LE MARCHÉ « GRANDS COMPTES » DE L'ASSURANCE CYBER

Structure du programme d'assurance Cyber du Groupe

- Les risques transférés vers le marché dans le cadre des programmes d'assurances des grands groupes rassemblent le plus souvent de nombreux acteurs du marché.
- La capacité assurée peut être mobilisée grâce à l'addition de lignes réunissant un ou plusieurs assureurs (ils interviennent alors en co-assurance, pilotés par l'apériteur).
- Le dispositif de prévention est présenté lors d'une réunion assureurs (Roadshow) et complété par les questions et questionnaires des assureurs.
- La forte crispation du marché en 2021 est caractérisée par une raréfaction des capacités disponibles en bas de programme, ce qui entraine de l'inflation. L'enjeu dans pareil contexte est de limiter sa dépendance aux assureurs de « premier niveau », en relevant la franchise et en concentrant la capacité disponible vers le haut du programme.
- Les assureurs les plus contraignants (primes élevées et/ou restrictions de garanties) sont repoussés vers le haut du programme.

Exemple de programme d'assurance