Quel avenir pour la Cyber-assurance ?

Présentation du rapport sur « La Cyber-assurance » du Groupe d'études Assurances de l'Assemblée Nationale et perspectives

Mardi 30 novembre 2021, Hôtel RITZ

Willis Towers Watson

GRAS SAVOYE
Willis Towers Watson

Sommaire

1. Présentation des enseignements du rapport et des principales recommandations
2. Le marché de l'assurance Cyber : tendances, attentes et perspectives
3. L'accompagnement des sociétés pour améliorer leur résilience aux risques Cyber : nécessité et enjeux
4. Echanges avec nos intervenants
5. Conclusion

Willis Towers Watson

GRAS SAVOYE
Willis Towers Watson

Introduction

Willis Towers Watson

GRAS SAVOYE
Willis Towers Watson

Nos intervenants

Valéria **FAURE-MUNTIAN**

- Députée de la Loire
- Membre de la Commission des Finances
- Présidente du Groupe d'amitié France-Ukraine
- Co-présidente du Groupe d'études « Assurances »
- Auteure du rapport sur la cyber-assurance du groupe d'études Assurances avec l'assistance de Monsieur Romain Dewaele.

Nos intervenants

Laure ZICRY

Responsable Cyber Europe du Sud, Willis Towers Watson

Guillaume DESCHAMPS

Directeur FINEX, Gras Savoye Willis Towers Watson

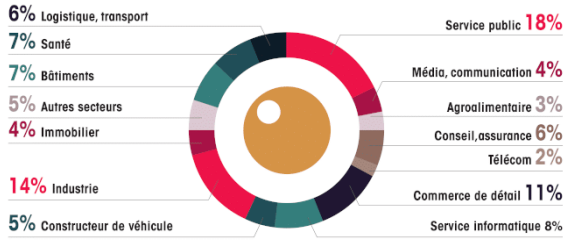
Ezechiel SYMENOUH

Responsable Cyber, Gras Savoye Willis Towers Watson

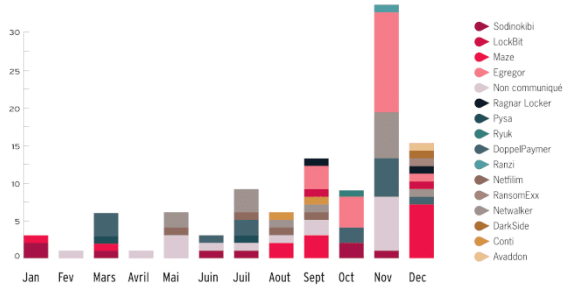
Rappel de l'environnement des risques Cyber en France

Un risque réel, croissant et qui menace tout type de société et d'organisation

// SECTEURS TOUCHÉS EN FRANCE EN 2020



// RÉPARTITION DES ATTAQUES DE RANSOMWARES EN FRANCE EN 2020



Source : EPITA, Livre blanc « Cybersécurités & Innovation », Edition 2020

Rappel de l'environnement des risques Cyber en France

Un risque identifié comme la première menace

10 PRINCIPAUX RISQUES EN FRANCE

Source : Allianz Global Corporate & Specialty.

Les chiffres représentent un pourcentage de toutes les réponses pour ce pays.

Participants : 66

Les chiffres ne totalisent pas 100% car 3 risques pouvaient être sélectionnés.

Classement		Pourcentage	Classement 2020	Tendance
1	Incidents cyber (ex : cyber crimes, défaillances informatiques, violation de données...)	50%	1 (49%)	=
2	Interruptions d'activités (y compris les perturbations de la chaîne logistique	44%	2 (48%)	=
3	Pandémie (ex : problématiques liées à la santé et à la main d'œuvre, restrictions de circulation...)	42%	NOUVEAU	▲
4	Incendie, explosion	24%	3 (35%)	▼
5	Atteinte à la réputation ou à l'image de marque	17%	9 (10%)	▲
6	Catastrophes naturelles (ex : tempête, inondation, tremblement de terre...)	17%	4 (30%)	▼
7	Défaillances de qualité, défauts de série, rappel de produits	15%	5 (18%)	▼
8	Évolutions macro-économiques (programme d'austérité, inflation/déflation...)	14%	NOUVEAU	▲
9	Évolutions législatives et réglementaires (ex : changement de gouvernement, sanctions économiques, protectionnisme, Brexit, désintégration de la zone Euro...)	12%	6 (17%)	▼
9	Risques politiques (ex : guerre, terrorisme, conflits sociaux...)	12%	7 (13%)	▼

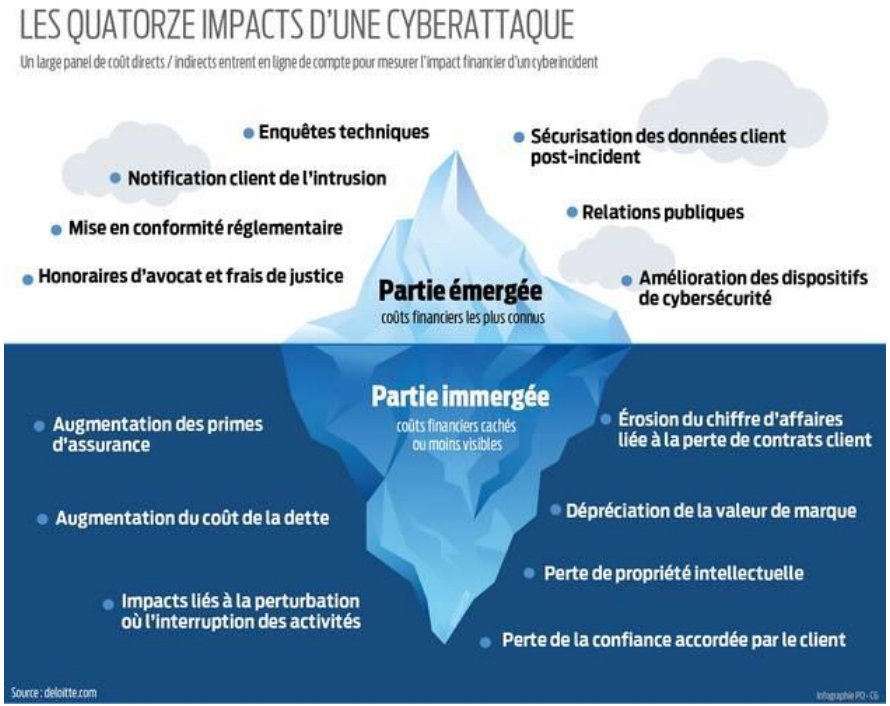
Top 5 risks to businesses

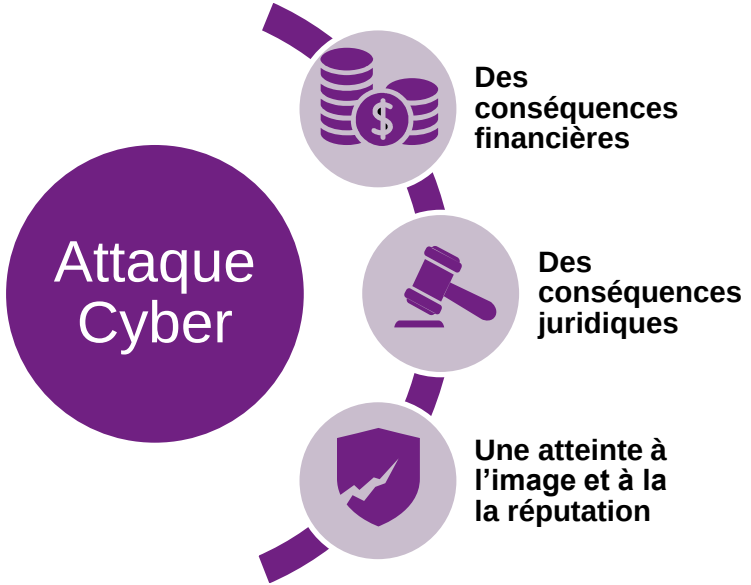
Rank	2021	2019	2018	2017	2016	2014	2013	2011
#1	Cyber-attack	Data loss	Risk of data loss / data breach	Regulatory and other investigations	Regulatory and other investigations and inquires	Regulatory and other investigations and inquires	Regulatory and other investigations and inquires	Regulatory and other investigations and inquires
#2	Data loss	Cyber-attack	Cyber-attack	Cyber-attack	Cyber-attack	Anti-Corruption Legislation (including the Bribery Act)	Criminal and regulatory fines and penalties	Criminal and regulatory fines and penalties
#3	Regulatory risk (including threat of fines and penalties)	Regulatory risk (including threat of fines and penalties)	Regulatory and other investigations	Risk of data loss / data breach	Risk of data loss / data breach	Criminal and regulatory fines and penalties	Anti-Corruption Legislation (including the Bribery Act)	Anti-Corruption Legislation (including the Bribery Act)
#4	Health & safety / environmental prosecutions	Litigation risk	Health and safety legislation	Criminal and regulatory fines and penalties	Criminal and regulatory fines and penalties	Risk of being sued abroad	Securities / Shareholder claims	Employment practices claims
#5	Risk of employment claims	Social media campaigns	Criminal and regulatory fines and penalties	Concerns in a post Brexit landscape	Anti-Corruption Legislation (including the Bribery Act)	Multiplicity of sanctions regimes and of affected countries	Risk of being sued abroad	Securities / Shareholder claims

Source : D&O Liability Survey 2021, Willis Towers Watson, April 2021

Rappel de l’environnement des risques Cyber en France

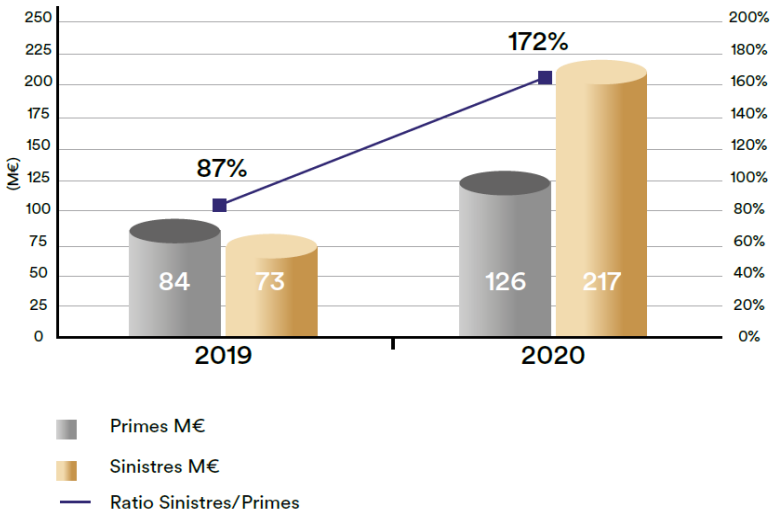
Un risque aux nombreuses conséquences (directes et indirectes)





Rappel de l'environnement des risques Cyber en France

Un risque pas suffisamment assuré ou assuré à des conditions « détériorées »



Source : Rapport LUCY, AMRAE

87 % des grandes entreprises mais seulement **8 %** des entreprises de taille intermédiaire ont souscrit une assurance cyber.

38 M€ hauteur moyenne de la couverture des grandes entreprises.

X 3 : augmentation de la sinistralité surtout en intensité : le montant global des indemnisations a été multiplié par 3, passant de 73 M€ en 2019 à 216 M€ en 2020.

+ 19 % pour les grandes entreprises et **+ 28 %** pour les ETI : augmentation des taux de primes entre 2019 et 2020.

167 % vs 84 % ratio Sinistres/Primes de 2020 vs celui de 2019.

Rappel de l'environnement des risques Cyber en France

Constat à ce jour

- **Un risque fortement présent** et identifié comme LA menace du moment
- **Une prise de conscience des conséquences d'un incident** ou d'une attaque cyber
- **Un cout significatif des conséquence** d'un incident ou d'une attaque cyber
- **Une meilleure appréciation du contenu et de l'intérêt d'une assurance Cyber**

Le besoin de disposer d'une Assurance Cyber

Mais

- **Un marché de l'assurance qui recadre la couverture des risques Cyber** (polices traditionnelles vs police Cyber « stand alone »)
- **Un processus de souscription dense, long, très technique et complexe**
- **Des exigences techniques (pre-requis) de plus en plus nombreuses**
- **Des franchises en forte hausse**
- **Des garanties « détériorées »**
- **Des conditions tarifaires en (forte) hausse**

1

Présentation des enseignements du rapport et des principales recommandations

Valéria Faure-Muntian

Willis Towers Watson

GRAS SAVOYE

Willis Towers Watson

1 Présentation des enseignements du rapport et des principales recommandations

Objectifs du rapport :

- **Il entend dresser un état des lieux de la situation de la cyber-assurance en France en vue de la structurer.**
- **Et proposer des voies d'amélioration jugées nécessaires dans un contexte toujours plus risqué pour les entreprises, qui peinent à se couvrir.**

Le contenu de ce rapport se décline sous la forme de **20 propositions** articulées autour de trois axes :

I. **Clarifier et définir le Droit** par l'adoption de définitions juridiques pour le cyber-risque et la cyber-attaque et prendre position sur la prise en charge de la rançon par les assureurs.

II. **Travailler sur la prévention et la défense** en renforçant l'écosystème français de la cybersécurité **et sur la résilience et la sensibilisation** des entreprises et des collectivités françaises à la menace.

III. **Développer le marché de la cyber-assurance**.

Les 20 recommandations du rapport :

I. Clarifier et définir le droit relatif aux cyber–risques et cyber-attaques

1) Adopter une définition commune du cyber-risque et de la cyber-attaque ;

2) Clarifier la législation en matière de paiement des rançongiciels ;

3) Préciser la législation relative au paiement des amendes administratives ;

4) Subordonner l'activation des garanties assurancielles au dépôt de plainte à la suite d'une cyber-attaque.

Les 20 recommandations du rapport :

II. Renforcer la résilience et la défense face aux cyber-risques

5) Promouvoir le dispositif *cybermalveillance.gouv.fr* auprès des entreprises et des collectivités ;

6) Créer un recueil anonyme des cyber-attaques frappant les entreprises géré par le GIP ACYMA (cybermalveillance.gouv.fr);

7) Renforcer les moyens humains, matériels et financiers du GIP ACYMA ;

8) Inciter les institutions européennes à instaurer un « small business act » de la cybersécurité en France et favoriser dans la commande publique des solutions souveraines ;

9) Allonger la formation des magistrats en matière de cybersécurité ;

Présentation des conclusions du rapport et des principales recommandations

Les 20 recommandations du rapport :

II. Renforcer la résilience et la défense face aux cyber-risques

10) Augmenter les moyens humains, financiers et matériels des services de la justice, de la police et de la gendarmerie chargés de la lutte contre la cybercriminalité ;

11) Sensibiliser au moins une fois par an les salariés des petites et moyennes entreprises aux risques cyber ;

12) Créer pour les collectivités, les administrations et les entreprises un prérequis en matière de cybersécurité ;

13) Créer au sein de l'État une agence nationale dédiée à des opérations cyberoffensives dans le secteur économique et industriel ;

Les 20 recommandations du rapport :

II. Renforcer la résilience et la défense face aux cyber-risques

14) Orienter directement les aides publiques aux collectivités et aux entreprises pour effectuer un audit de cybersécurité et à se doter d'un dispositif de cybersécurité ;

15) Imposer aux entreprises qui travaillent pour et/ou avec l'État et/ou des OIV /OSE à se doter d'une police d'assurance cyber ;

16) Développer un écosystème en rapprochant les assurances françaises des entreprises de cybersécurité françaises.

Les 20 recommandations du rapport :

III. Développer le marché de la cyber-assurance

17) Inciter à la création en Europe d'un mécanisme d'évaluation des offres de cyber-assurance ;

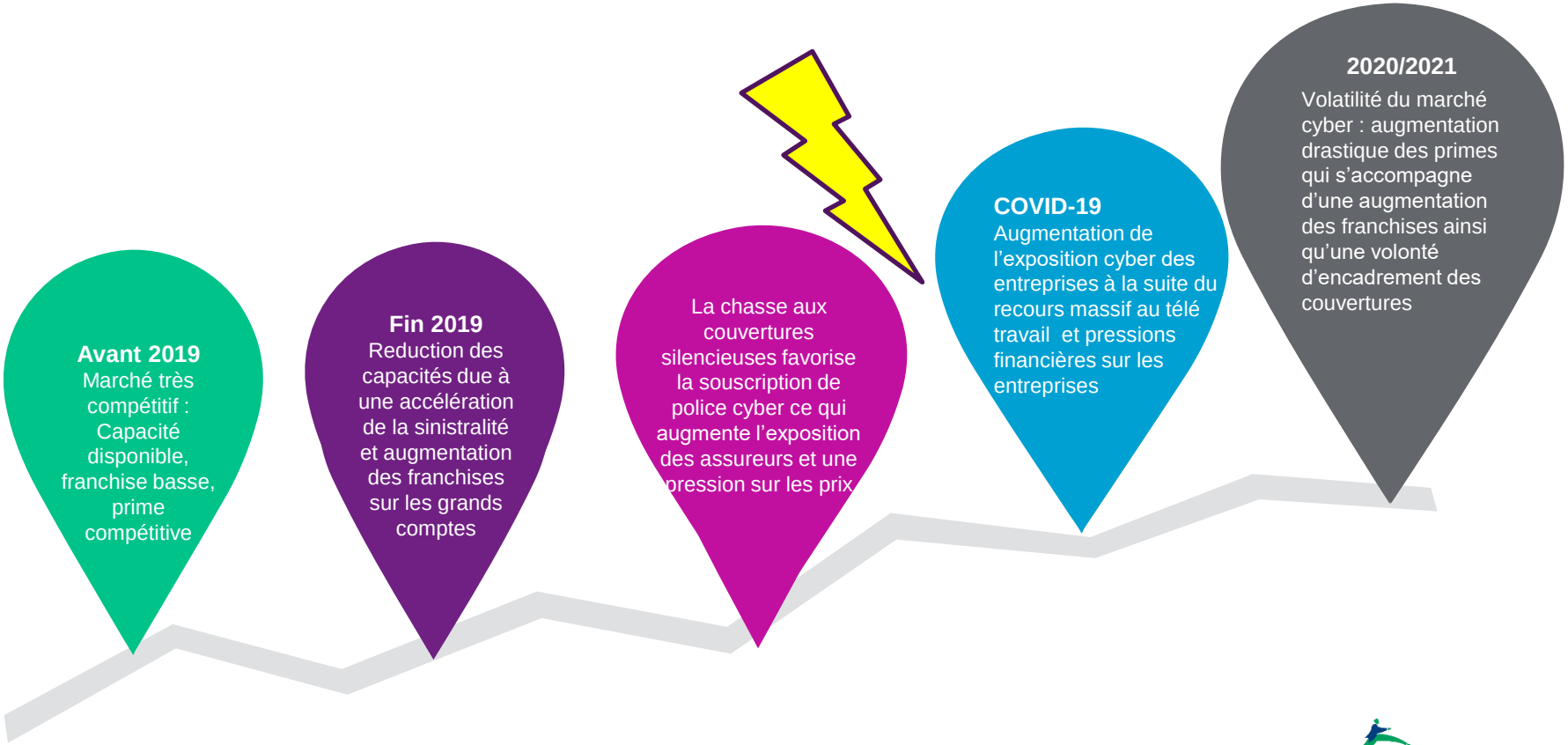
18) Harmoniser à l'échelle française puis européenne les critères d'analyse des cyber-risques entre les assureurs ;

19) Créer une nouvelle branche d'assurance dédiée à la cyber-assurance ;

20) Développer des solutions hybrides de cybersécurité et de cyber-assurance pour les petites et moyennes entreprises et les collectivités.


2
Le marché de l'assurance Cyber : tendances, attentes et perspectives
Willis Towers Watson
GRAS SAVOYE
Willis Towers Watson

2 Le marché de l'assurance Cyber : tendances, attentes et perspectives

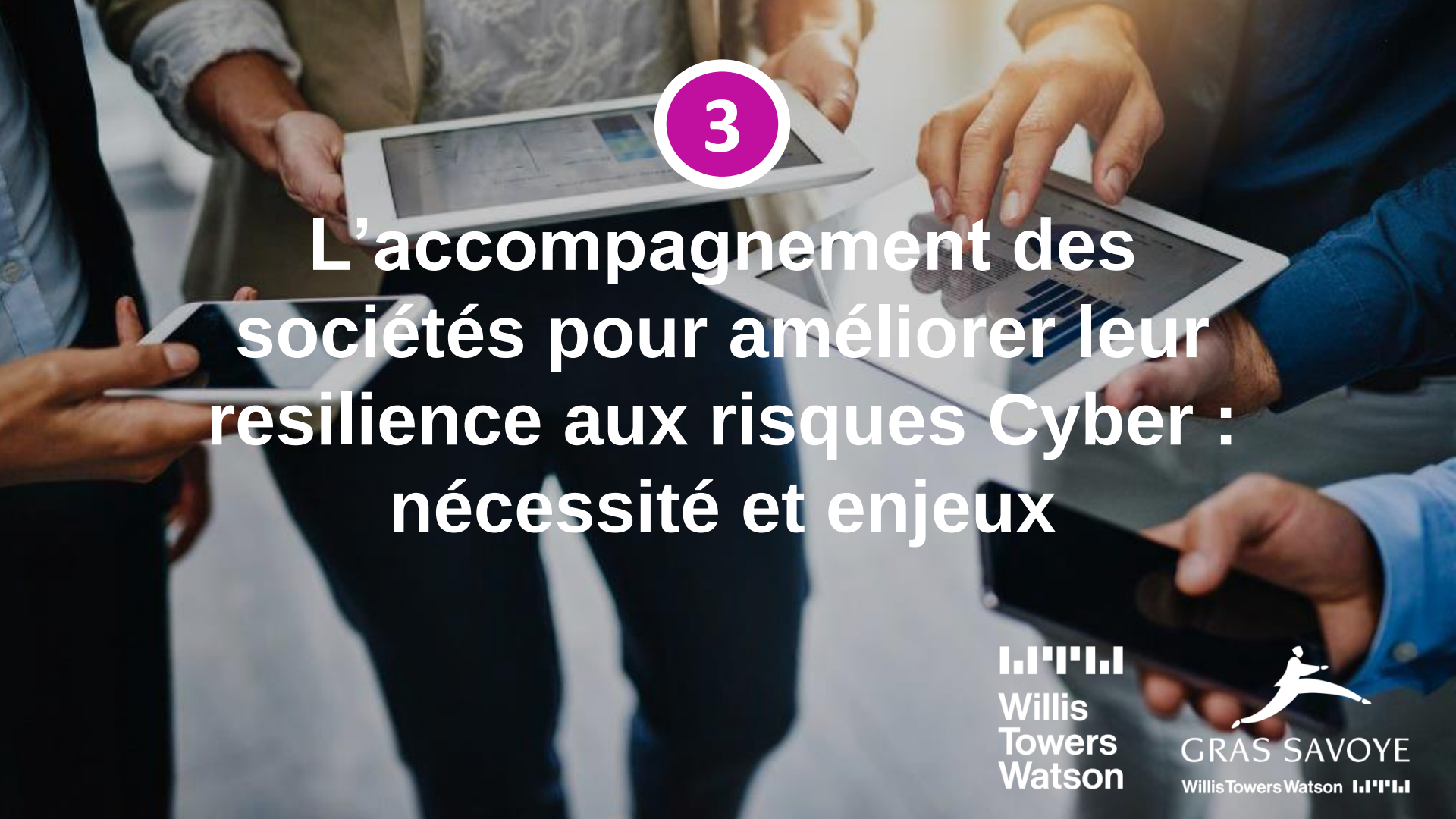


2 Le marché de l'assurance Cyber : tendances, attentes et perspectives

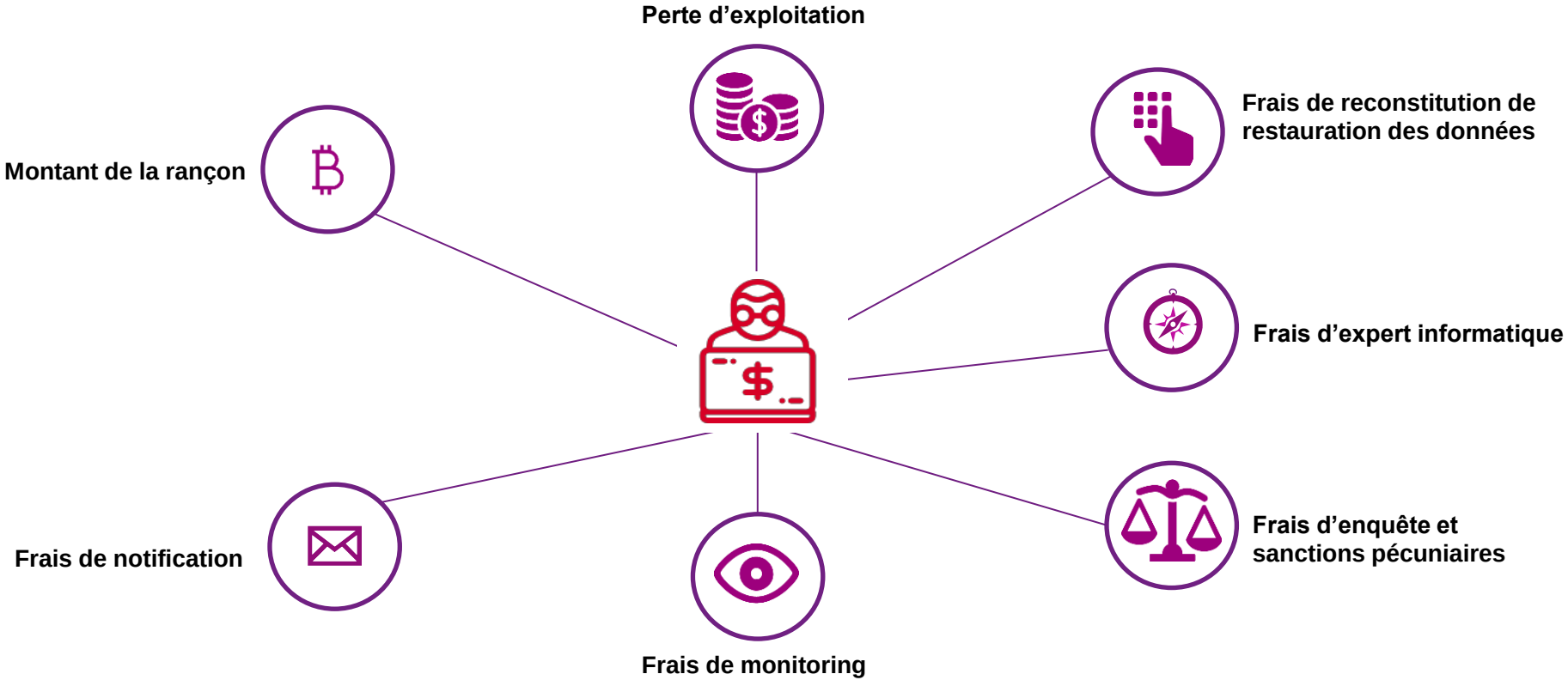
Capacité	Souscription / Garanties	Sinistralité	Primes & Franchises
Contraction	**Limitation**	**Aggravation**	**Forte Augmentation**
• Forte réduction des capacités offertes par assureur (2019 : 25M€, 2020 : 15M€, 2021 : 5-10M€), • **en Primary**: raréfaction des acteurs, manque de concurrence • **en Excess** : points d'attachement de plus en plus élevé (une grande majorité attachent à 50M€) • Questionnaire Ransomware obligatoire • Des appétits de souscription qui sont revus au niveau mondial et révisés continuellement	• Information de souscription : une politique de souscription très encadrée avec des minimum requis. Une sélection très drastique des dossiers en fonction de leur niveau de maturité et des contrôles mis en place. • Restrictions de couvertures : Clause de Coassurance ou Quotité Non Garantie sur les événements Ransomware et/ou sous limite. • Deux approches différentes : Limit reducing ou Loss reducing Approach	• Rapport sinistres/primes fortement détérioré depuis 2019. • **La Fréquence de l'Intensité** • Augmentation du nombre de Ransomwares et des coûts engagés par l'Assuré pour atténuer et restaurer les SI après l'attaque. • Monitoring mondial : Assureurs directement touchés par l'évolution défavorable de la sinistralité.	• Augmentation des primes des traités de réassurance. • Primes et franchises de nouveau revues à la hausse (franchises différenciées selon le type de couvertures difficiles à obtenir). • Peu ou pas de marge de négociation, très forte volatilité.

2 Le marché de l’assurance Cyber : tendances, attentes et perspectives

Sécurité Informatique	Agilité	Captives
Renforcement / Mise à niveau	**Innovation**	**Transfert**
• Standard de Sécurité NIST (National Institute of Standards and Technology : 5 piliers **1.Identifier** : Identifier les types de menaces et tous les actifs potentiellement à risque. **2.Protéger** : Analyser la meilleure façon de protéger tous les actifs identifiés. **3.Détecter** : Définir comment les menaces contre les actifs seront détectées. **4.Répondre** : Décrire les mesures clés pour répondre aux menaces détectées. **5.Récupérer** : Définir comment réparer l'infrastructure touchée et maintenir la sécurité.	• Repenser la politique de transferts de risques • Montages alternatifs : ✓ Vertical Quota Share, ✓ Excess SIR, ✓ Fronting + lettre de crédit	• Pour les Captives déjà en place : De plus en plus de captives impliquées dans la couverture des risques cyber • Etude de faisabilité de mise en place de Captives pour optimiser les coûts et lutter contre le manque de capacité ou d’acteurs tant en primary qu’en excess.


3
L’accompagnement des sociétés pour améliorer leur resilience aux risques Cyber : nécessité et enjeux
Willis Towers Watson
GRAS SAVOYE
Willis Towers Watson

3 Les coûts d'une attaque par ransomware : la double extorsion change les règles d'indemnisation



3 Les principaux enseignements des attaques par ransomware : une évolution de l'état de la menace

Compromission de l'active Directory. L'attaquant possède des comptes d'administration du domaine dans la majorité des cas.

Courriels d'hameçonnage restent un vecteur d'infection largement utilisé.

Des attaquants toujours plus rapide. 3 jours entre l'accès initiale et le déploiement du ransomware

Faille de sécurité ou défaut de configuration sur les services d'accès à distants (Accès RDP, VPN, Citrix, Pulse…) exploités par les pirates informatiques.

Les attaques de la supply chain sont à surveiller. La supply chain IT pourrait être le nouveau vecteur d'infection des pirates informatiques.

3 Les principaux pré-requis des assureurs : les mesures exigées (“Must Have”)

Outil de gestion des accès à privilège (PAM)

Un outil de gestion des accès privilégiés permettant de surveiller les comptes ayant un accès privilégié aux actifs clés.

Endpoint Detection & Response (EDR)

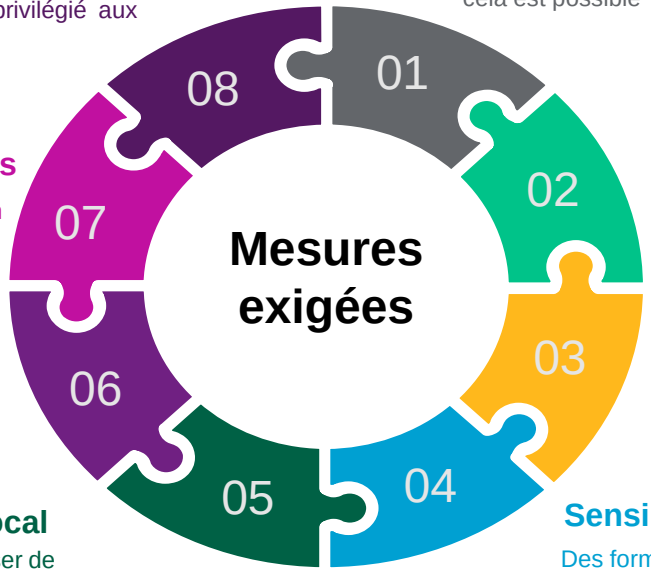
Mis en place sur tous les serveurs lorsque cela est possible

Gestion d’actifs informatiques

Inventaire de l'environnement à l'aide d'un outil de gestion des actifs.

Authentication multi-facteur (MFA)

Mis en place et requis pour tous les accès distants au réseau de l'entreprise ainsi que pour toutes les connexions à Office365.



Centre d’Opération de Sécurité (SOC)

Surveillance du réseau.

Procédures de sauvegarde

Sauvegarde hors ligne ou solution de sauvegarde alternative rendant impossible la suppression des sauvegardes existantes

Privilèges d’administrateur local

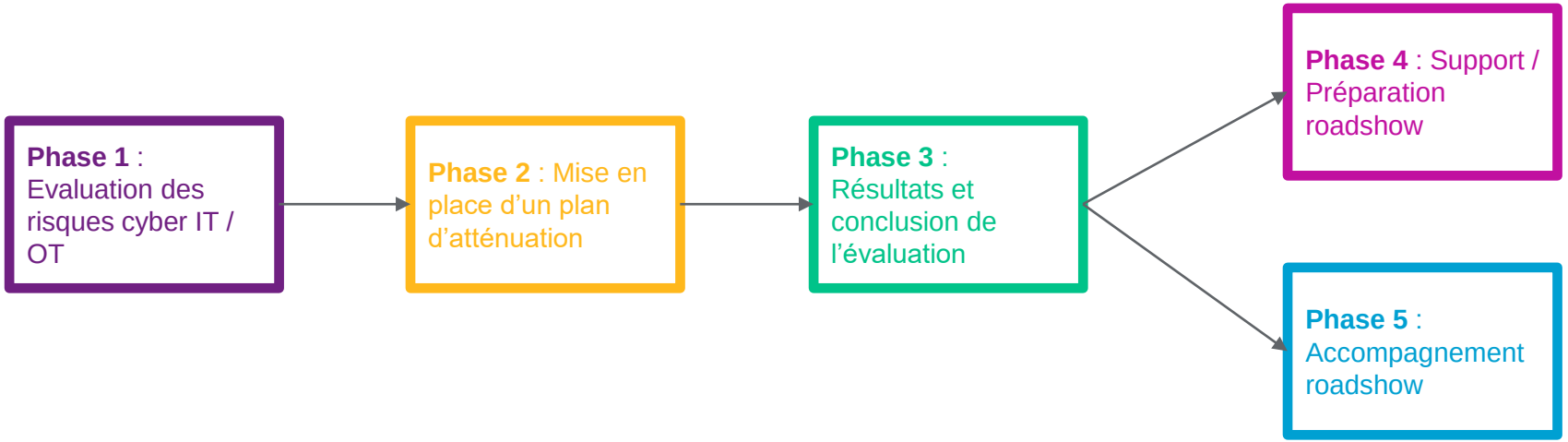
Les administrateurs locaux doivent disposer de comptes distincts pour leur utilisation quotidienne et pour les tâches nécessitant un accès administrateur..

Sensibilisation des employés

Des formations et/ou des campagnes de sensibilisation sont prévues et obligatoires pour tous les utilisateurs de technologies informatiques, au moins sur une base annuelle.

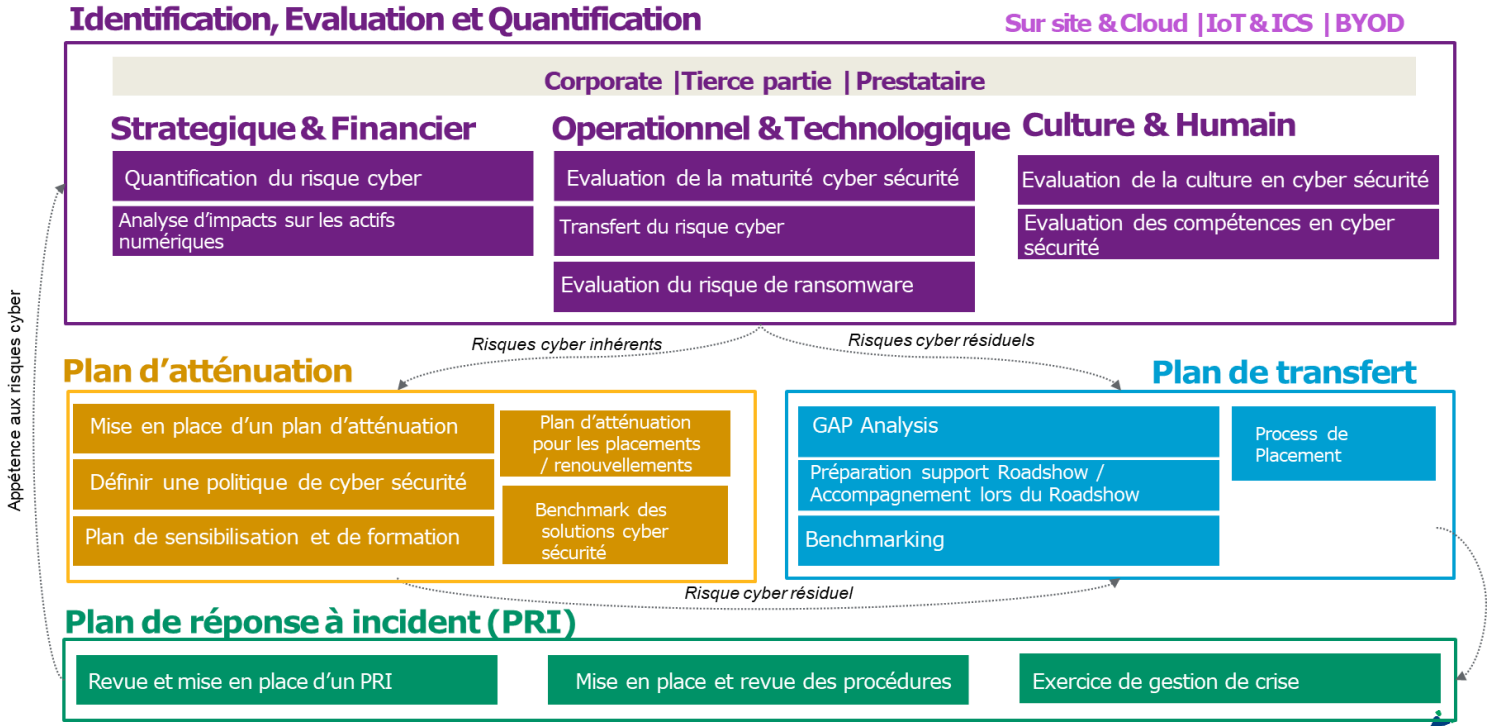
3 L’accompagnement des sociétés pour améliorer leur resilience aux risques Cyber : nécessité et enjeux

Une offre intelligente pour accompagner les entreprises à répondre aux pré-requis des assureurs :



3 L'accompagnement des sociétés pour améliorer leur resilience aux risques Cyber : nécessité et enjeux

Une approche Entreprise [Cyber] Risk Management (ERM) pour améliorer votre cyber résilience




4
Echanges avec nos intervenants
Willis
Towers
Watson
GRAS SAVOYE
Willis Towers Watson


5
Conclusion
Willis
Towers
Watson
GRAS SAVOYE
Willis Towers Watson


Merci pour votre participation !
GRAS SAVOYE
Willis Towers Watson