Risques Cyber

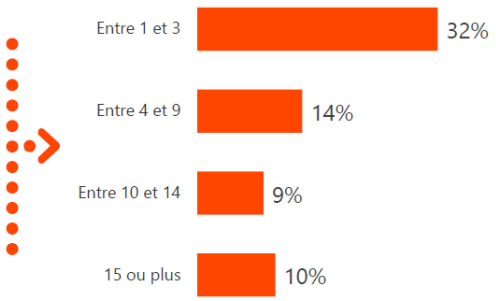
Commission Responsabilité Civile AMRAE

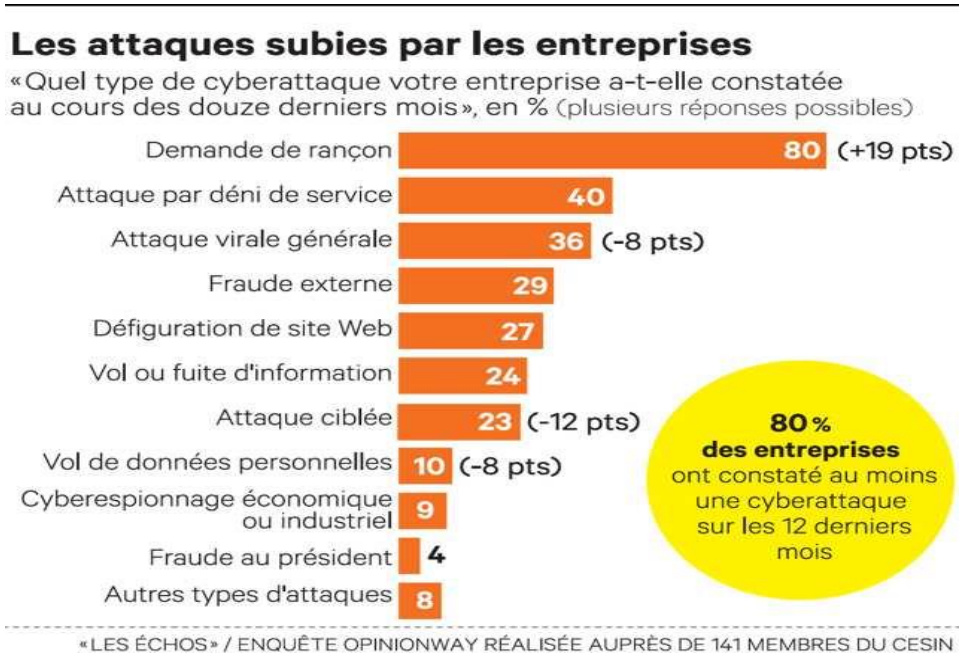
06 mars 2020

Willis Towers Watson

Quelques chiffres sur les risques cyber en France

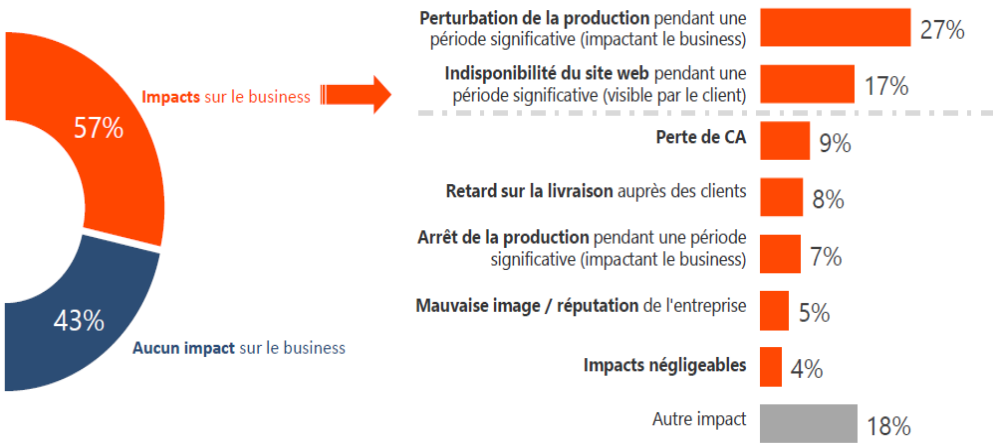
65%
des entreprises ont constaté au moins une cyber-attaque

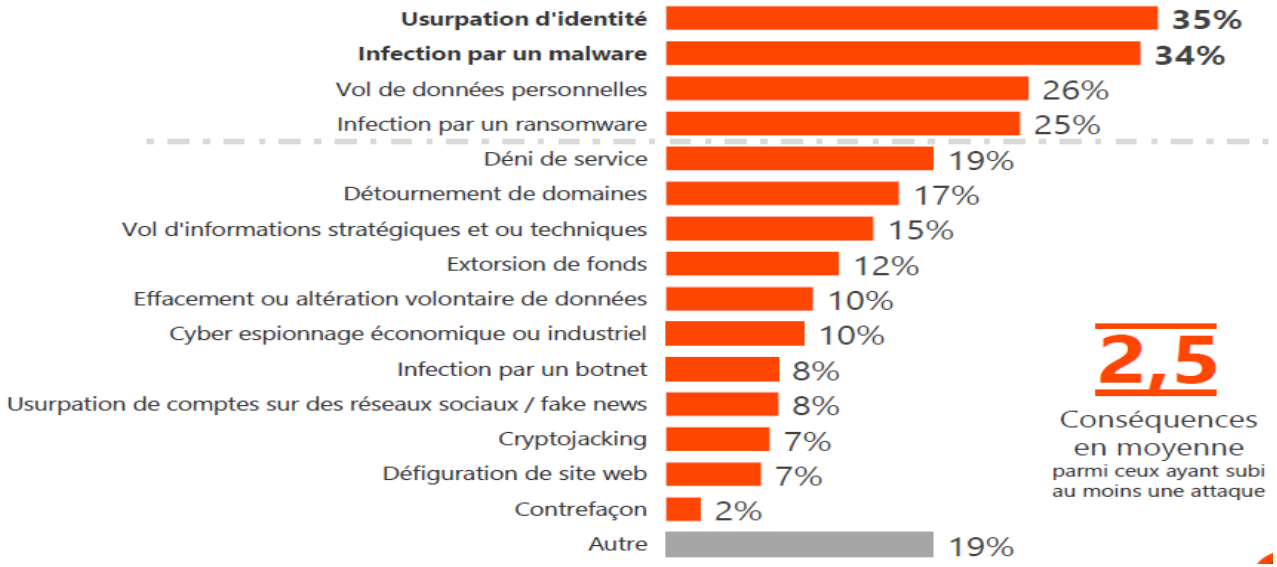




Tous les secteurs d'activités sont touchés

Quelques chiffres sur les risques cyber en France





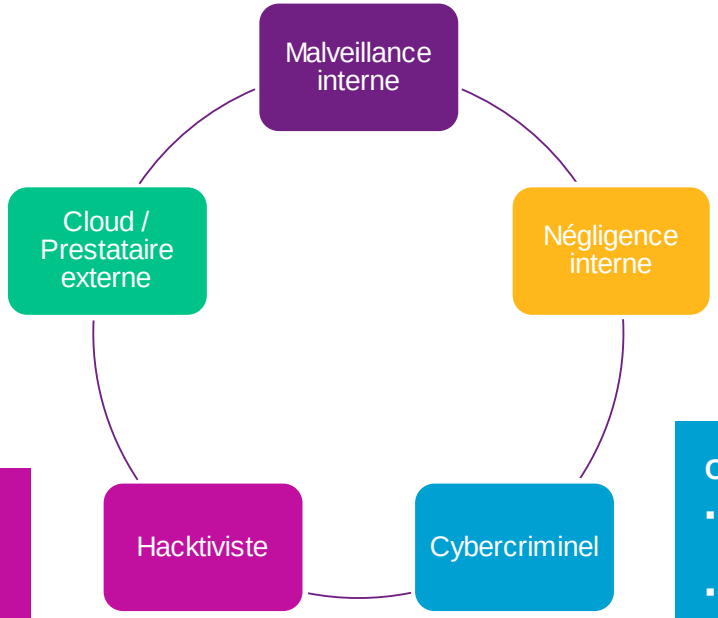
Exposition aux risques cyber : Les différentes menaces

Malveillance interne

- Insuffisance des contrôles des accès et surveillance des comportements pour détecter les menaces internes

Cloud / Prestataire externe

- Incitation croissante pour les initiés à abuser de l'accès aux données sensibles à des fins de gains financiers
- Les actuels ou anciens employés mécontents peuvent exploiter des « portes dérobées »
- Vol de propriété intellectuelle des tiers
- Violation de sécurité – perte de données clients sensibles
- L'indisponibilité des l'infrastructures peut entrainer une interruption des activités



Négligence interne

- Salariés victimes d'attaques exploitant les contrôles de sécurité traditionnelles (ex: phishing)
- Les salariés qui n'adoptent pas la «culture de sécurité » , trouverons toujours un moyen de contourner les contrôles de sécurité

Hacktivistes

- L'intention est de perturber et/ou embarrasser la cible
- Les motivations sont inconstantes et imprévisibles
- Attaques massives par DDoS

Cybercriminel

- La patience est une vertu. Les techniques d'intrusion évoluent
- Industrialisation – Tous types de données sont présents sur le dark web
- Prolifération des plateformes mobile et des BYOD – créateur de nouveaux vecteurs

Risques Cyber : définition & conséquences

Qu'entend-on par Cyber risques ?

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, et conséquences d'une atteinte au système informatique.

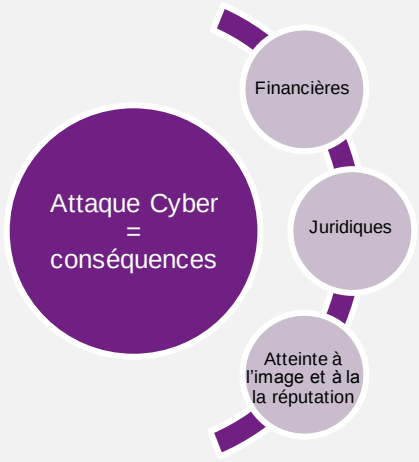
Définition

- **Atteintes aux données numériques**
  - Vos données nécessaires à l'activité
  - Les données appartenant :
    - Aux tiers.
    - A vos collaborateurs.
    - A vos clients.
    - A vos fournisseurs, sociétés partenaires, etc.

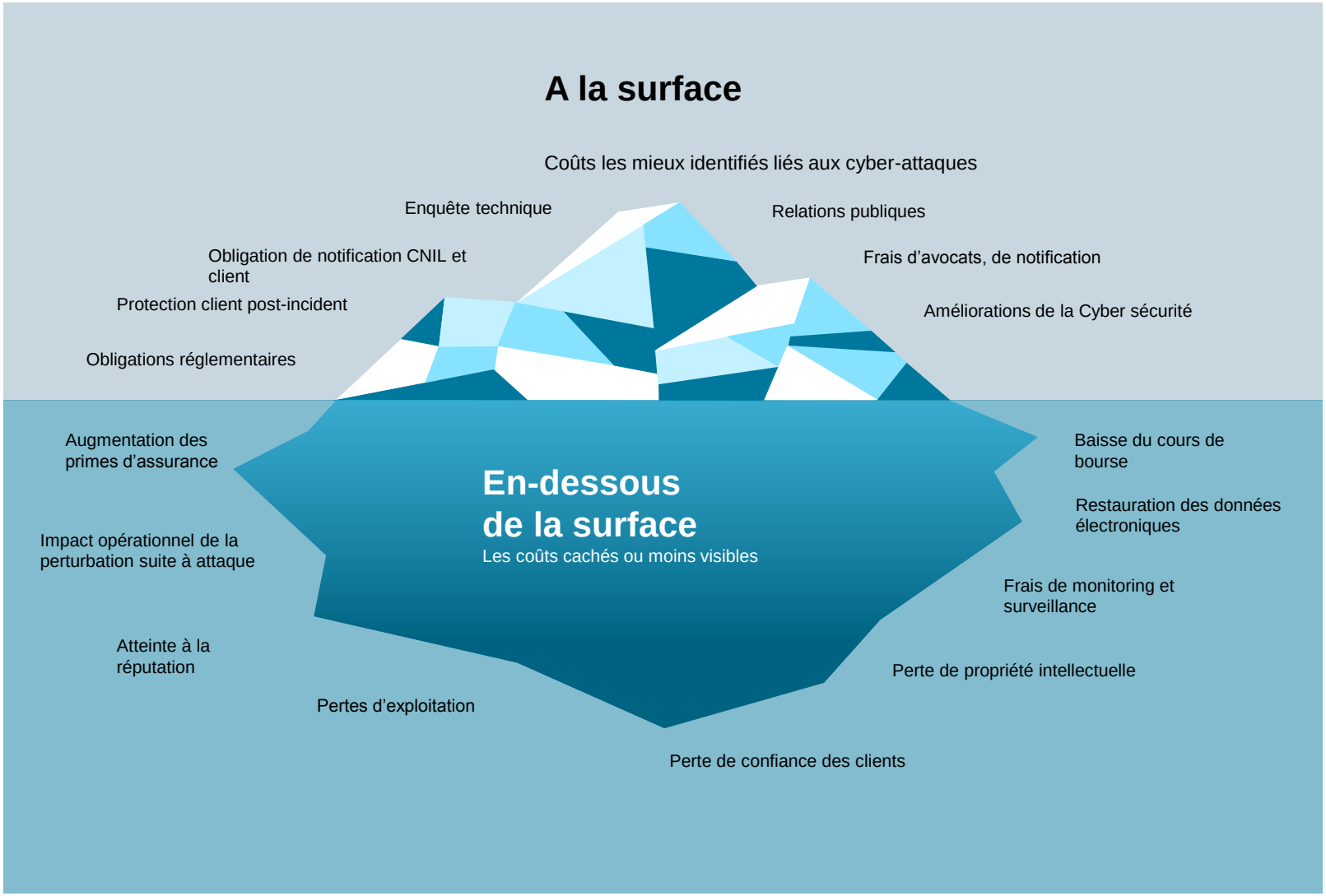
- **Atteintes au système informatique**
  - **Intrusion** dans les systèmes informatiques.
  - **Interruption** des systèmes informatiques.
  - **Contamination** des systèmes (virus, bombe logique, etc.).
  - **Utilisation illégale** des systèmes et du réseau.

Conséquences

Une Cyber-attaque peut générer une crise majeure pouvant remettre en cause la pérennité même de l'entreprise.



Risques Cyber : quels impacts ?



Quel est l'objet d'un contrat d'assurance cyber ?

Le contrat d'assurance Cyber a pour objet :

- De prendre en charge les frais engagés par ou pour le compte de l'assuré, en cas d'Incident réel ou allégué découvert pendant la période d'assurance : volet « **Gestion de la Crise** ».
- De garantir l'Assuré contre les Frais de défense et les Conséquences Pécuniaires résultant de Réclamations formulées à son encontre pendant la Période d'Assurance ou la Période Subséquente : volet « **Responsabilité** ».
- De prendre en charge les frais ou pertes qui ont un impact sur l'Assuré, en cas d'Incident réel ou allégué découvert pendant la période d'assurance : volet « **Dommage** »

… Les 3 grands volets d'une police d'assurance Cyber

Gestion de crise	**Responsabilité Civile**	**Dommage**
Attaque par Deni de service	**Interruption du système informatique**	**Ransomware**
Atteinte aux données	**Virus**	**Erreur Humaine**

Focus sur le volet Responsabilité d'une police d'assurance Cyber

L'Assureur prend en charge, les sommes suivantes engagées par ou pour le compte de l'Assuré avec l'accord préalable de l'Assureur.

La police couvre :

- Les frais de défense
- Les réclamations
- Les sanctions pécuniaires si légalement assurables

Suite à une :

- Atteinte aux données
- Atteinte médiatique
- Un manquement à l'obligation de notification
- Prestataire d'externalisation

Volet Responsabilité Civile

Couverture lorsque l'assuré est responsable:

Devant une Autorité Administrative:

- Frais d'enquête
- Sanctions pécuniaires (Seulement si assurables)

Vis à vis des tiers résultant d'une/d'un :

- Atteinte aux données
- Atteinte au système informatique
- Atteinte médiatique
- Manquement à l'obligation de notifier
- Incident chez un prestataire externe

Quels événements liés à une attaque Cyber pourraient être couverts par une police RC?

Avant la prise de conscience du « Silent Cyber »

Les garanties étaient silencieuses car
* Pas de garanties spécifiques
* Pas d'exclusions spécifiques
(quelque fois le virus)

Couvertures des
Dommages Corporels
Dommages Matériels
DIC
DINC

Après la prise de conscience du « Silent Cyber »

Volonté de supprimer les Couvertures Silencieuses avec 2 méthodes :
* Insertion de garanties spécifiques
* Insertion d'exclusions spécifiques
* Les 2

Couvertures des
Dommages Corporels
Dommages Matériels
DIC
~~DINC*~~

* Les DINC sont couverts dans le contrat Cyber

Décoder les risques Cyber

Une démarche structurée et complète

Evaluer : Analyse de l'exposition

Identification
Identifiez les risques qui affectent votre organisation

Quantification
Mesurez l'impact sur votre bilan d'un sinistre cyber suite à une atteinte aux données ou réseau

Stratégie
Mettez en place un plan d'action pour créer une culture de risque cyber

Protéger : Atténuer & Transférer

Sensibilisation
Sensibilisez vos collaborateurs aux risques cyber

Intégration
D'une culture du risque solide dans votre entreprise

Assurance
Se couvrir avec une assurance adaptée à vos besoins et en lien avec votre portefeuille

Autofinancement
Déterminer le montant optimal à retenir en impliquant éventuellement une captive

Surmonter : Résister & Se renforcer

Gestion des sinistres
Nos spécialistes sinistres vous guident pour faire intervenir vos contrats d'assurance et obtenir les indemnisations les plus larges possibles.

Gestion de crise
Nous travaillons avec vos équipes d'intervention pour coordonner et exécuter vos plans d'intervention en cas d'incident.

Expertise d'assuré
Nos experts quantifient votre exposition avant l'incident et les pertes après incident en cas d'incident cyber.

Continuité des activités
Développer des stratégies qui minimisent les interruptions d'activité et la perte de capital.


Risque Humain

+


Risque Financier

+


Risque Technologique

Comprendre et analyser l’exposition Cyber

Grâce à des séries d’entretiens et aux bases de données sinistres Cyber Willis Towers Watson:

- Identifier les risques et leurs conséquences
- Développer des scénarios pertinents compte tenu des spécificités de chaque clients
- Prendre en compte les dispositifs de maîtrise des risques existants et axes d’amélioration

Libellé du scénario	Description / Causes	Dispositifs de maîtrise des risques	Axes d'amélioration
Compromission d'un système clé	Découverte tardive d'une corruption du système d’information. Interruption complète de toute activité pendant 9h générant d'importants surcoûts De nombreuses conséquences sont répertoriées notamment lié aux applications métier et d’exploitation.	Segmentation des accès Plan de continuité d’activité Plan de reprise d’activité	Renforcement des conditions et limites d’accès
Perte de matériel sensible	Perte d'un outil périphérique (clé USB, smartphone, etc.) contenant des informations sensibles sur d'importants clients. Les données de clients corporate et leurs chantiers sont publiées sur internet provoquant des réactions négatives du grand public et d'importantes réclamations des groupes.	Cryptage des outils périphériques Non consolidation de données sensibles	Formation des cadres sur les cyber risk

Comprendre et analyser l'exposition Cyber

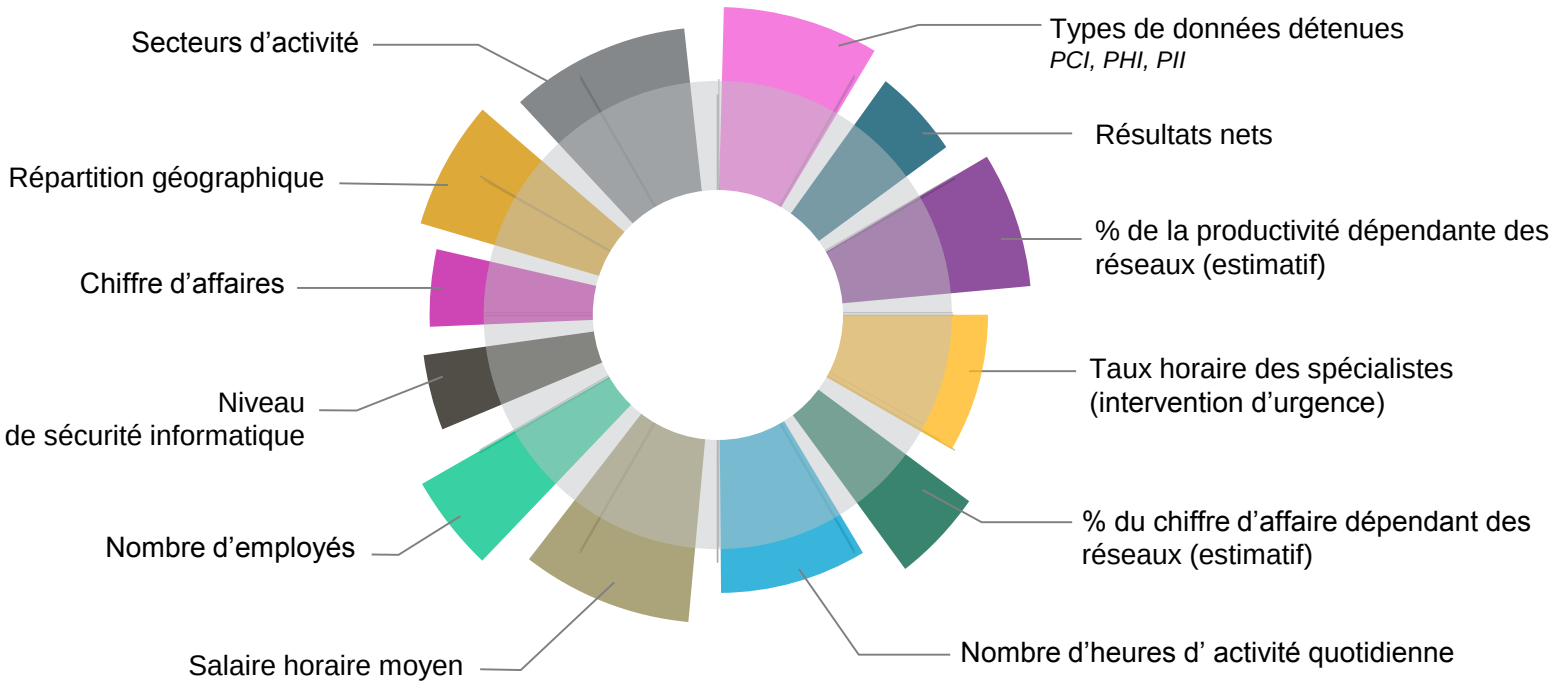
Etudier l'assurabilité des scénarios, leurs fréquences et leurs impacts respectifs

Risques étudiés				Police impactée					
Risque	**Description du scénario**	**Fréquence**	**Montant (K€)**	**DAB**	**Cyber**	**Fraude**	**RC**	**RCMS**	**Non assurable**
Perte de matériel sensible	Perte d'un outil périphérique (clé USB, smartphone, etc.) contenant des informations sensibles sur d'importants clients. Les données de clients corporate et leurs chantiers sont entièrement publiées sur internet provoquant des réactions négatives du grand public et d'importantes réclamations des groupes. Le Groupe subit une amende au nom du RGPD.	X fois tout les X ans	X K€		✓ X K€		✓ X K€	✓ X K€	✓ X K€
Incendie d'un Data Center	Un défaut électrique se produit en engendrant un incendie dans le siège au milieu de la nuit. La structure est totalement détruite par l'incendie. Conséquences sur le voisinage	X fois tout les X ans	X K€	✓ X K€	✓ X K€		✓ X K€		
Fraude interne	Un administrateur profite de son accès pour modifier des comptes bancaires, dont le sien, les créditant de plusieurs milliers d'euros. L'affaire est médiatisée et les comptes crédités dévoilés exposant de nombreuses personnes publiques sensibles avec leurs détails bancaires. Certaines personnes touchées par l'affaire se retournent en justice pour atteinte à la vie privée.	X fois tout les X ans	X K€		✓ X K€	✓ X K€			

Comprendre et analyser l'exposition Cyber

Intrusions et Vol de données

Interruption de systèmes



Comprendre et analyser l'exposition Cyber

Return period (years)

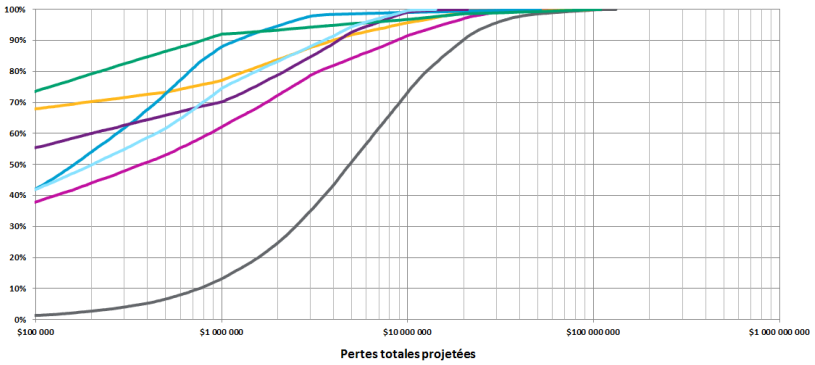
Fréquence – Temps moyen (en années) entre des réclamations d'un montant donné.

Percentile

Probabilité que la perte totale projetée en une année soit inférieure à une valeur donnée.

Total Cost

Perte totale projetée avant application du programme assurantiel.



Amounts in €M

Return Period (Years)	Percentile	Total Cost
3 in 4	25,0%	2,03
1 in 2	50,0%	4,87
1 in 4	75,0%	10,54
1 in 5	80,0%	12,59
1 in 10	90,0%	19,74
1 in 20	**95,0%**	**27,83**
1 in 50	**98,0%**	**41,66**
1 in 100	99,0%	61,05
1 in 200	99,5%	80,37
1 in 500	99,8%	97,82
1 in 1000	99,9%	102,10
	Mean	**8,55**

Illustration – Tableau de projection des pertes

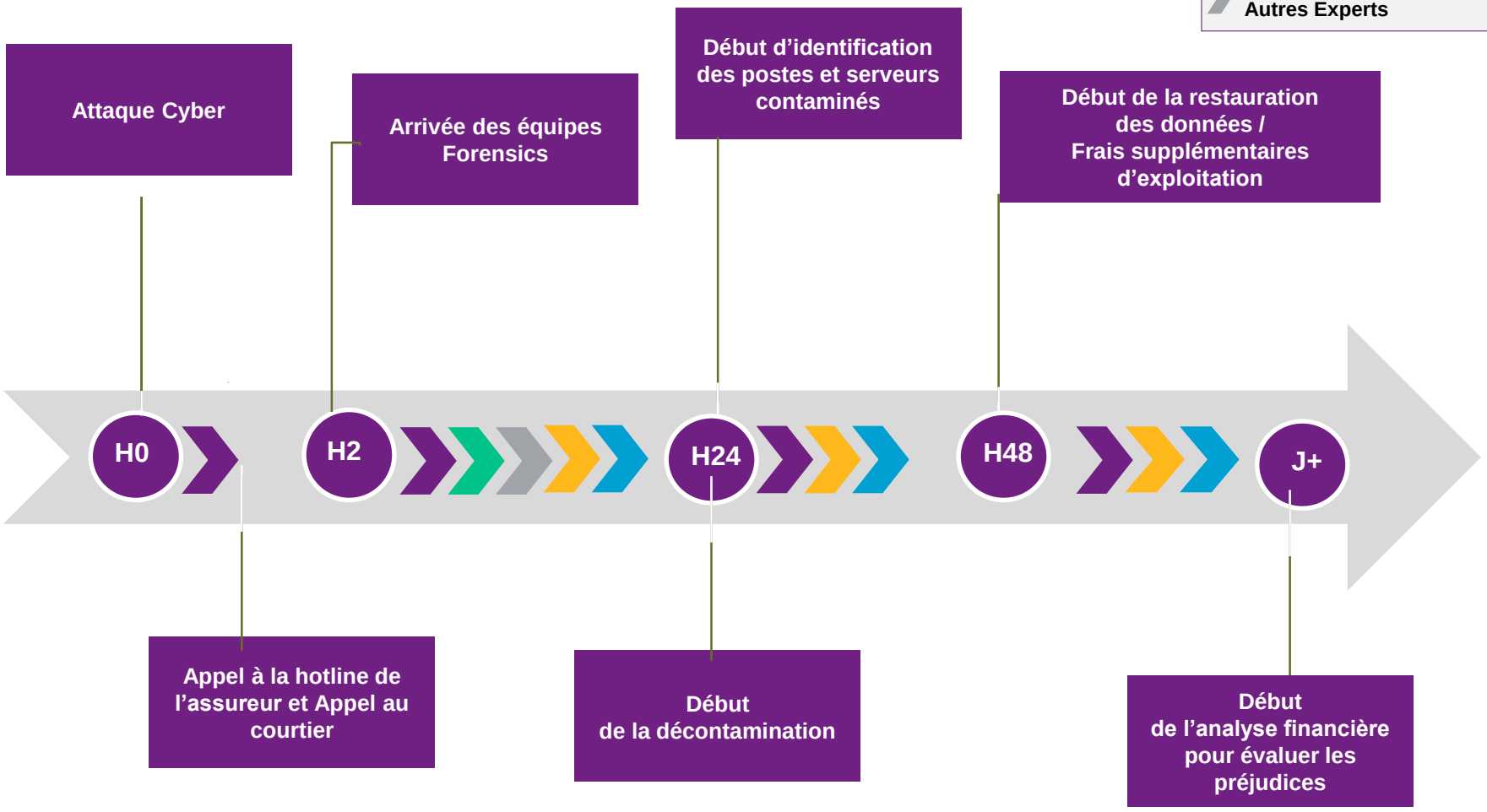
- Pertes projetées pour un risque en fonction de 6 scénarios identifiés.
- Exemple de lecture - Les pertes découlant d'une fuite ou d'un vol de données PI seront probablement supérieures à 16,8 millions de dollars dans 10 % des cas

Amounts in $m

Gross Results

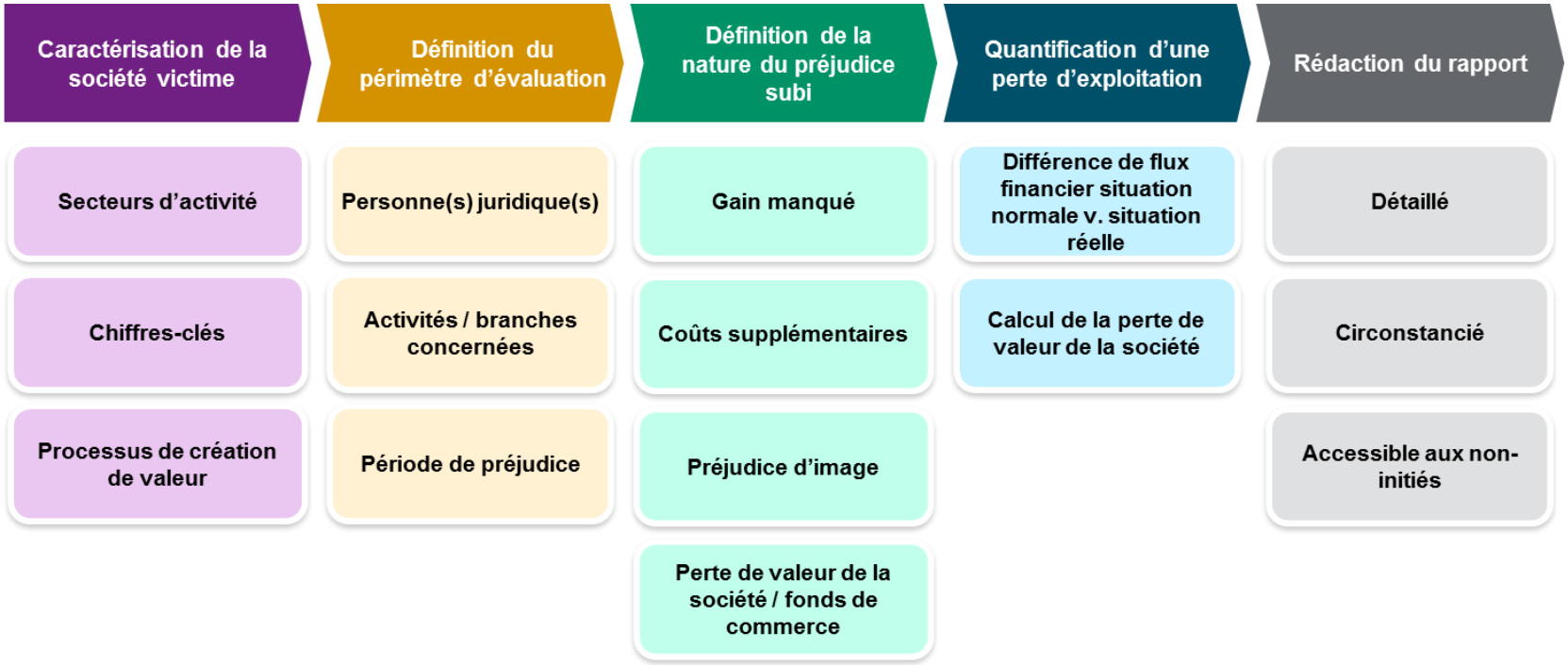
Exceedence Probability	Total Cost	Violation of ethical standards	Breach or theft of PII data	Talent	Agility	Relevance	Consumer Expectations
75.0%	11.97	-	-	-	-	-	-
50.0%	**22.94**	**0.14**	**1.65**	**3.95**	**-**	**0.97**	**-**
25.0%	38.39	2.19	8.11	10.79	9.70	4.47	0.01
10.0%	62.99	28.37	16.80	17.20	20.45	9.30	0.41
0.5%	318.50	213.22	136.61	30.09	41.36	27.45	3.89
Mean	**33.59**	**10.80**	**7.34**	**6.12**	**6.09**	**3.05**	**0.19**
Std Dev	**48.44**	**38.60**	**26.33**	**7.39**	**9.16**	**4.71**	**0.85**

La gestion de la crise



Evaluer les préjudices – Forensic Accounting & Complex Claims

- **Simplifier** le processus de réclamation afin d'accélérer la reprise de l'activité normale.
- **Quantifier** les montants des sinistres à l'aide d'une méthodologie solide et alignée avec celles des experts de l'assureur
- **Récolter** tous les documents pertinents à l'analyse
- **Réduire** au minimum la perturbation des activités du client avec des avances de fonds aussitôt que possible
- **Collaborer** avec les directions techniques et d'indemnisations ainsi que les experts de l'assureur pour simplifier le processus et mener au mieux la réclamation à son terme
- **Participer** à des réunions pour justifier la méthodologie de calcul des pertes et répondre à toute demande supplémentaire
- **Examiner** les différends commerciaux en prenant en compte l'importance des relations d'affaires existantes

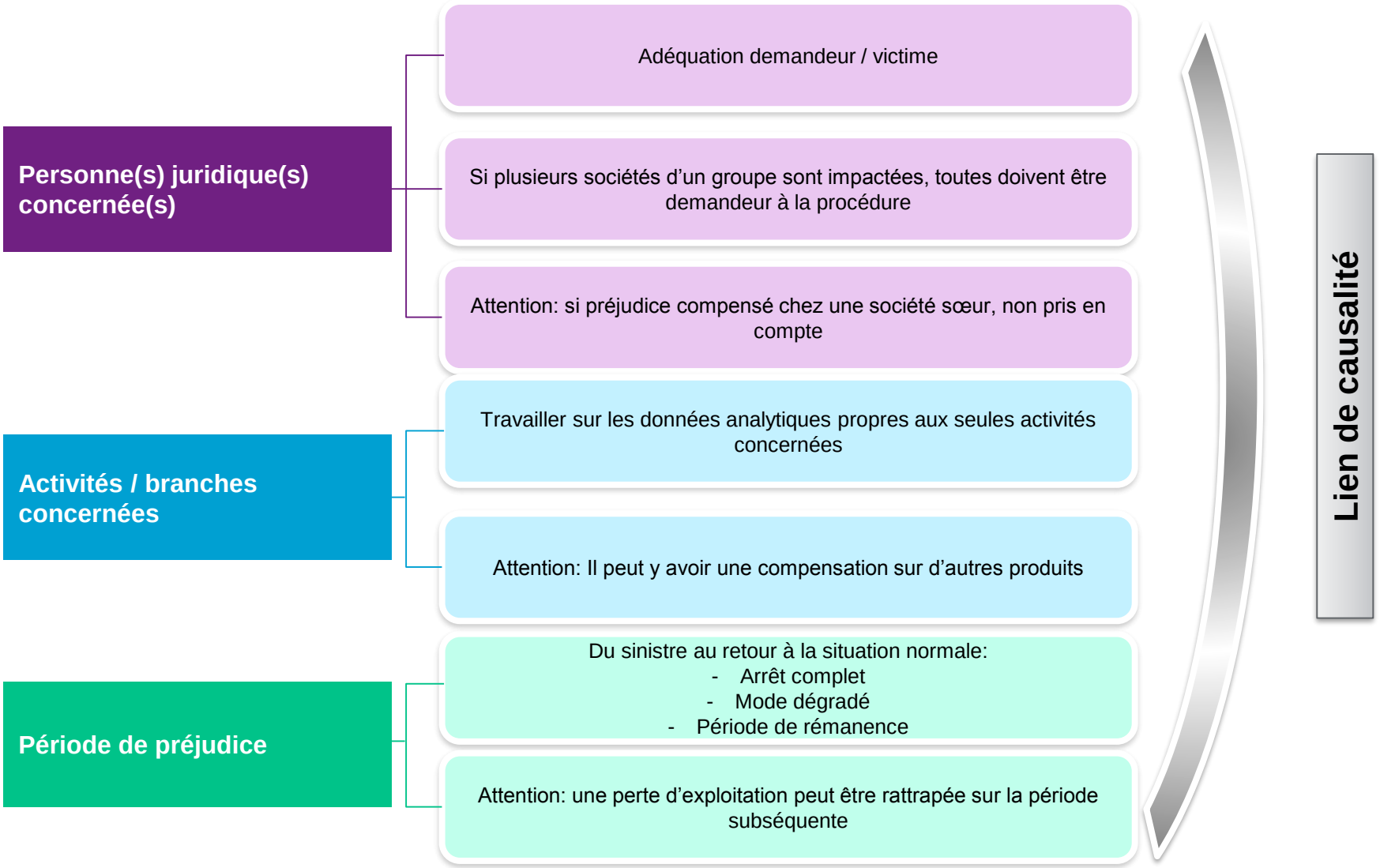


Evaluer les préjudices – Forensic Accounting & Complex Claims
Phase 1 : Caractérisation de la société victime

Données à collecter	Intérêt de ces données
▪ **Secteur d'activité** : production, distribution, services, etc.	▪ **Comprendre** le processus de génération de valeur
▪ **Chiffres-clés** : CA, principaux soldes intermédiaires de gestion	▪ **Challenger** l'importance du préjudice subi par des contrôles de cohérence simples
▪ **Organigramme** : appartenance à un groupe ?	▪ **Comprendre** les interactions avec d'autres sociétés du groupe
▪ **Documents comptables** : Organisation comptable et financière	▪ **Comprendre** l'organisation comptable de la société : Présence d'une comptabilité analytique, par branche, par site …
▪ **Les données techniques** : nécessaire collaboration entre expert financier et expert technique	▪ **S'assurer** du lien de causalité entre le sinistre et la perte financière

Evaluer les préjudices – Forensic Accounting & Complex Claims

Phase 2 : Définition du périmètre d'évaluation



Evaluer les préjudices – Forensic Accounting & Complex Claims

Phase 3 : Définition de la nature du préjudice subi

Illustration - *Les principaux types de préjudice*

1 Gain manqué

- **Réalisé**
- **A venir**

Perte de chance = gain manqué x % de probabilité que la chance de le réaliser se produise**.**

2 Frais supplémentaires

- **Respect du lien de causalité**
- **Problème des coûts fixes de salariés**

3 Préjudice d'image

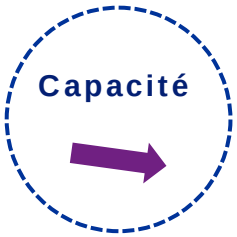
- Ramené à un gain manqué futur et/ou frais supplémentaires (ex : communication)
- Méthode de la redevance implicite
- Méthode de la dépréciation de l'investissement

4 Perte de valeur d'une société

- Appréciée par les méthodes classiques d'évaluation (comparables, DCF)

Attention aux doublons avec le gain manqué !

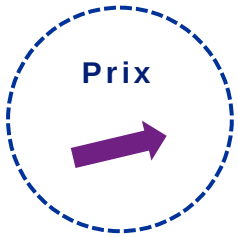
Etat du marché de l'assurance Cyber en France (capacité et tendance)



20 assureurs sur le marché français

Capacité théorique : environ **600M€**

Capacité disponible : environ **225M€**



La France reste un des marchés les plus compétitifs d'Europe

Pour les renouvellements 2020 **des majorations** :

- entre **10%** et **30%** pour les comptes non sinistrés
- plus **100%** pour les comptes sinistrés

Différents niveaux de franchise en fonction de la taille de l'entreprise et de son exposition

Les garanties restent homogènes mais **l'interprétation des textes assureurs reste aléatoire**

Evolution continue de notre texte Cyber afin de clarifier les garanties pour nos clients

Sélection des risques par les assureurs, selon le niveau de sécurité des entreprises en fonction de leurs enjeux informatiques

Willis Towers Watson