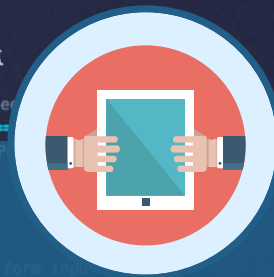




Cabinet Devorsine

COURTIER EN ASSURANCE • NANTES • PARIS



Les Cybers risques

Réalités et couvertures

Programme de la réunion



Introduction

Quels risques pour les entreprises ?



Les couvertures assurancielles

Comment se couvrir contre les risques Cyber ?



Exclusions et points de vigilance

Fraude, passé connu, titres financiers ...



Comparatif CYBER vs. FRAUDE

Un contrat Cyber ne couvre pas contre les risques de fraude



Conclusions

Pourquoi AIG ? Quel est le process de souscription ? Questions/Réponses

Qu'entend-on par Cyber Risque ?

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

Données nécessaires à l'activité de l'assuré, des collaborateurs, appartenant aux clients, aux fournisseurs, partenaires, prestataires



RGPD



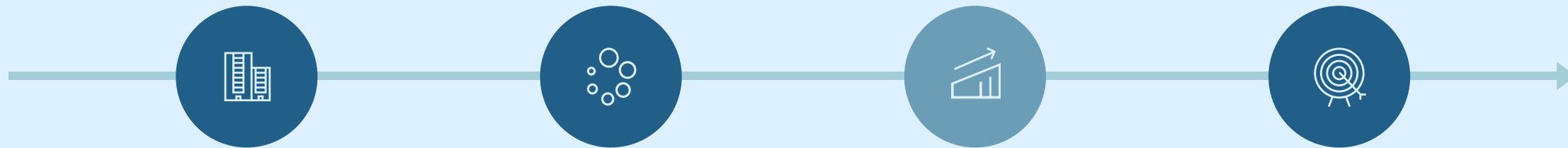
Les atteintes aux systèmes informatiques

Intrusion, interruption, contamination des systèmes informatiques (virus, phishing ...). Utilisation illégale des systèmes et du réseau ...



Fraude

Les entreprises très exposées



Gestion des données

Le volume de données échangées et conservées par les entreprises à considérablement augmenté

Cloud / Collaboratif

Les fonctionnements et les outils de travail évoluent rapidement

Rentabilité des attaques

-Simplicité
-ROI élevé

Sécurité / Prévention

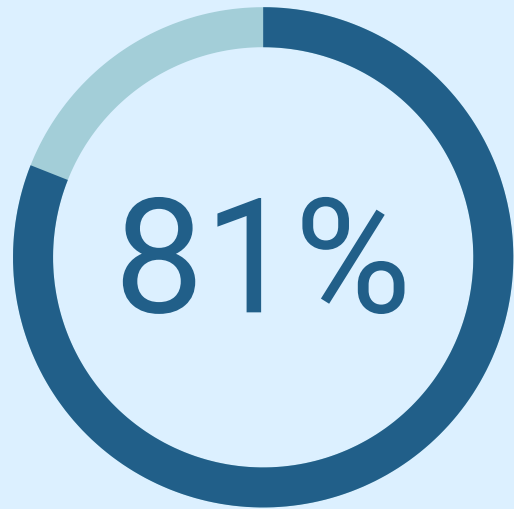
Erreur humaine

Malgré des systèmes de sécurité ambitieux, aucune entreprise n'est à l'abri (erreur humaine, phishing ...)

La question ce n'est plus de savoir si cela va arriver, mais
Quand ? et Comment s'y prépare-t-on ?

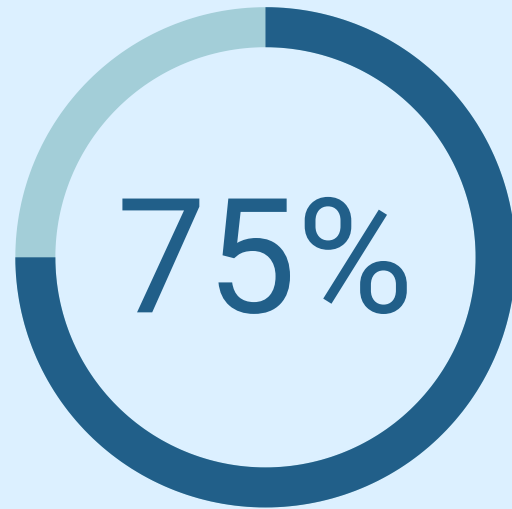


Quelques chiffres



Entreprises visées

8 entreprises Françaises sur dix ont été visées par une cyberattaque en 2015.
sondage OpinionWay



Erreur humaine

75% des incidents de cybersécurité dus à des collaborateurs



Notification (en €)

25€ est le coût moyen d'une notification (clients + régulateurs)
AIG



Coût moyen

300 000 € - 1000 salariés
1,3M€ . +5000 salariés.
NTT Com Security



9 semaines

Temps nécessaire avant de reprendre l'activité à 100%
NTT Com Security

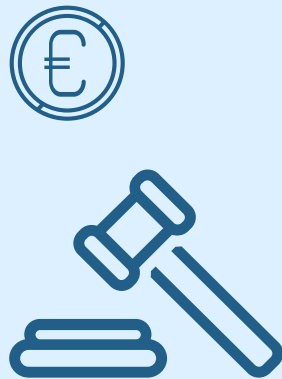
[Article de Microsoft sur le sujet](#)

Les coûts d'une cyber-attaque



Communication

Communication de crise, Frais de notification, Frais de monitoring des données affectées

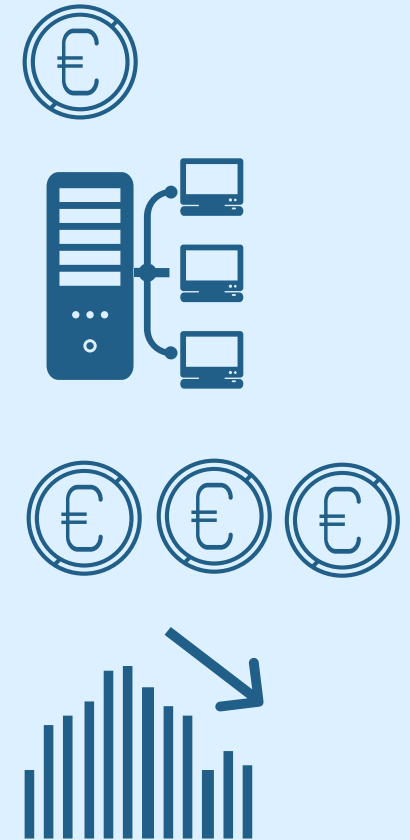


Rançon, sanctions

Rançon en cas d'extorsion. Pénalités et sanctions infligés par les régulateurs
Honoraires d'avocats

Systèmes IT

Frais d'expertise IT des systèmes endommagés, Frais de réparation et de restauration des données



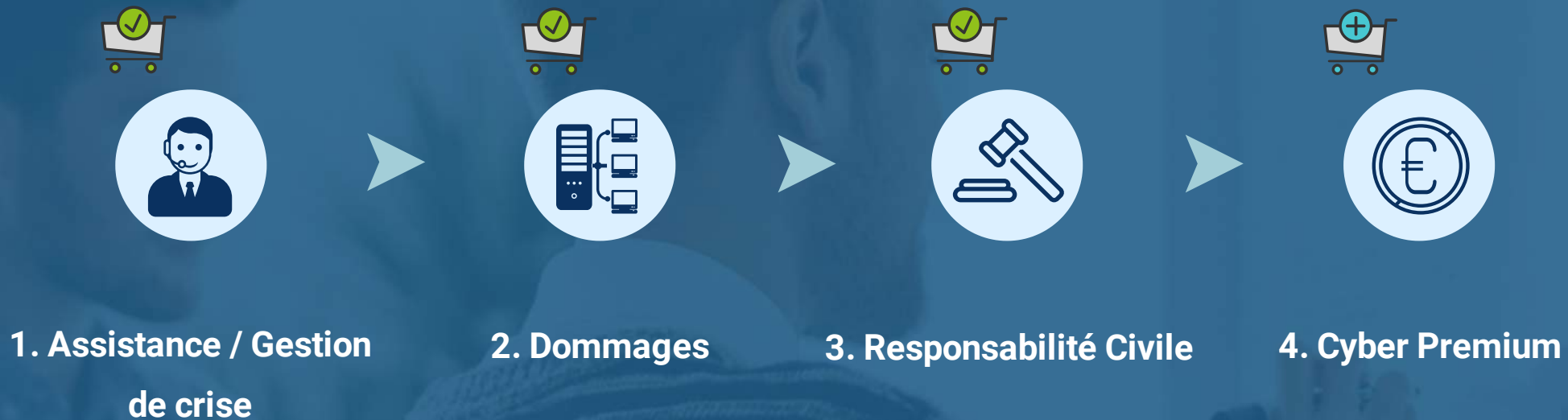
Pertes financières

Domages & intérêts
Domages à la réputation
Interruption d'activité,
...



Cyber Assurance

Une solution complète de gestion des Cyber-Risques combinant "*Transfert de risque*" et "*Services*"

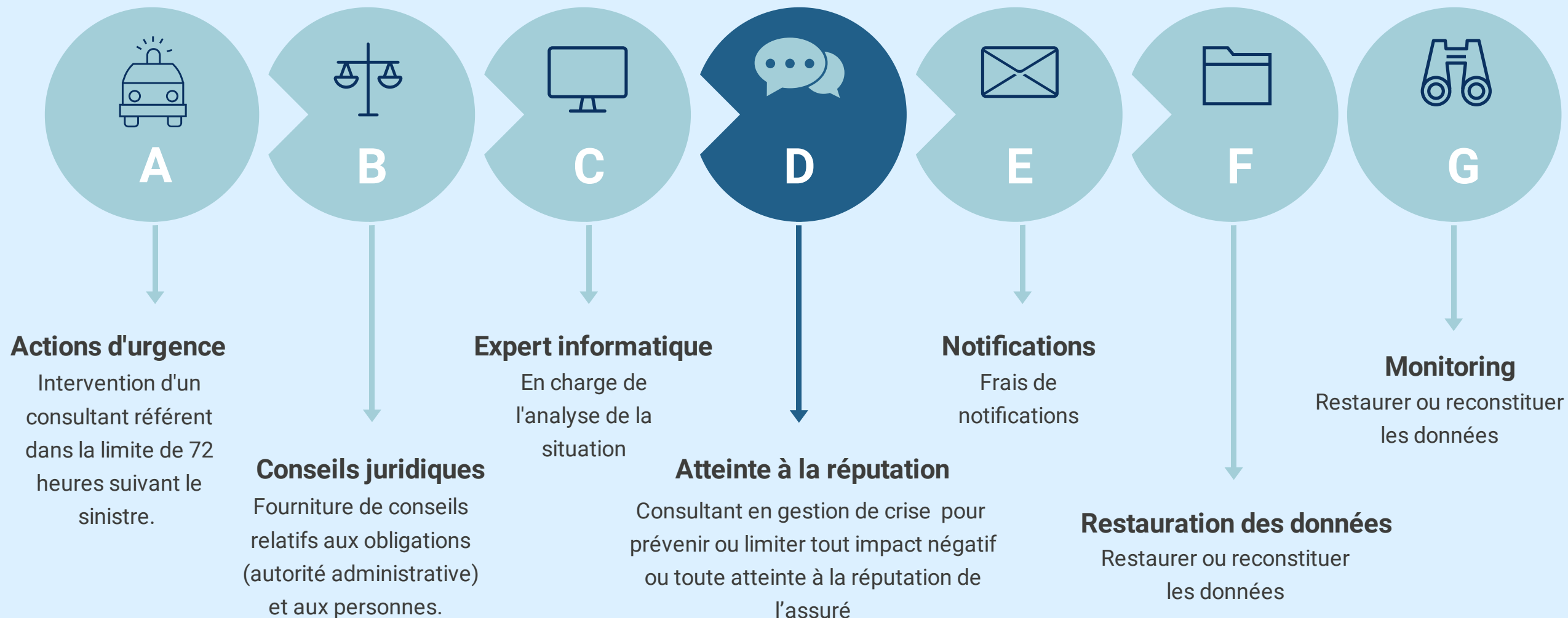


Ce document est non contractuel et a été réalisé à titre d'information uniquement. Il ne saurait reprendre exhaustivement l'ensemble des conditions, garanties, franchises et exclusions figurant aux conditions générales.

Pour mieux comprendre - Accès vidéo



Les garanties Assistance / Gestion de crise



Ce document est non contractuel et a été réalisé à titre d'information uniquement. Il ne saurait reprendre exhaustivement l'ensemble des conditions, garanties, franchises et exclusions figurant aux conditions générales.

Pour mieux comprendre - Accès vidéo



Les garanties "Dommages"

Enquête et sanctions (administrative)

Frais de défense dans le cas d'une enquête administrative
Sanction pécuniaire légalement assurables

Cyber Extorsion

Sur accord du consultant référent missioné dans les mesures d'urgence



Pertes d'exploitation

L'assureur prend en charge les pertes d'exploitation subies par la société souscriptrice
- dans un délai de 120 jours après l'évènement
- dans un délai de 90 jours suivant la résolution de l'évènement assuré



Les garanties "Responsabilité Civile"

L'assureur prend en charges les conséquences pécuniaires et frais de défenses suite à une réclamation résultant de toute réclamation imputable à:



Atteintes aux données



Atteinte à la sécurité
du système
informatique



Manquement à
l'obligation de
notifications



Sous traitant



Média



Frais d'atténuation
du risque



La garantie optionnelle "Cyber Premium"

Il s'agit d'un volet "Fraude" très léger qui couvre, exclusivement, les pertes pécuniaires directes subies suite à l'accès ou l'utilisation non autorisée du système informatique ou téléphonique.



Fraude téléphonique

L'assureur prend en charge le cout de la **surconsommation téléphonique** due par la société souscriptrice à son opérateur télécom suite à :

- l'accès non autorisé au système téléphonique ; ou
- l'utilisation non autorisée du système téléphonique situé(s) dans les locaux professionnels de la société souscriptrice.



Fraude informatique

L'assureur prend en charge les **pertes pécuniaires directes** subies par la société souscriptrice suite à :

- l'accès non autorisé au système informatique ; ou
- l'utilisation non autorisée du système informatique de la société souscriptrice par un tiers.



Exclusions et points de vigilance

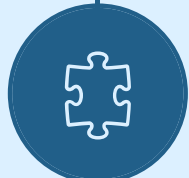
Sont recensés, ci-dessous, les principales exclusions figurant au contrat ainsi que les points de vigilance. Cette liste est non exhaustive.



Panne | Des systèmes informatique, électrique, téléphonique ...



Faute intentionnelle



Le passé connu



Propriété Intellectuelle | Divulcation ou du détournement de secrets de fabrique, de contrefaçon de brevets ...



Les titres financiers



Les pénalités contractuelles



Les frais n'incluent pas les salaires et rémunérations. | Principe de la Perte d'exploitation



La fraude | Hormis l'option Cyber Premium, la fraude n'est pas couverte dans le contrat Cyber



Contrat Cyber vs. Fraude

Un contrat Cyber ne couvre que les pertes pécuniaires directes d'un accès non autorisé aux systèmes informatiques de l'entreprise

CYBER

Garantir l'atteinte aux données et aux systèmes informatiques

L'assuré et les tiers



1. Assistance / Gestion de crise



2. Dommages



3. Responsabilité Civile



Objet du contrat ?



Qui est couvert ?



Garanties

FRAUDE

Couvrir les pertes financières

L'assuré uniquement

Pertes pécuniaires, fonds détournés, rançons

Contrat Cyber vs. Fraude

Les garanties d'un contrat Fraude



Préjudice pécuniaire direct suite à

Détournement de fonds, de marchandises ou de biens

Pertes indirectes / Frais

- Frais supplémentaires d'exploitation et de procédure
- Frais de reconstitution d'informations,
- Frais de restauration de la capacité du réseau;
- Frais d'atteinte à la réputation
- Frais de procédure
- Intérêts et pénalités

Indemnisations des pertes

- Quel qu'en soit l'auteur (employé ou tiers, avec ou sans collusion entre eux) y compris dirigeant de filiales, sans restriction quant à sa qualité ou ses pouvoirs
- Quel qu'en soit le moyen (informatique ou non)
- Quel qu'en soit le but (gain personnel ou malveillance)

Pourquoi nous travaillons avec AIG

Sur les contrats CYBER et FRAUDE



Expérience

Leader des couvertures CYBER et FRAUDE depuis plus de 20 ans.
A l'origine de l'introduction de ces contrats en France dès 2009



Gestion des sinistres

Dispose d'une équipe dédiée à la gestion des sinistres
Un contrat qui s'appuie sur les prestations d'un partenaire de renommée mondiale (InQuest) et des consultants de haut niveau



Des garanties évolutives et adaptées

- Intervention des prestataires 24/24 tout au long de l'année
- Garantie des sanctions pécuniaires prononcées par une autorité administrative
 - Cyber extorsion
- Perte d'exploitation sans sous-limite et garantie pendant le temps de l'interruption d'accès aux données et pendant 90 jours suivant la résolution de l'évènement



Cabinet Devorsine

COURTIER EN ASSURANCE • NANTES • PARIS

Merci pour votre écoute

Des questions ?



laurent@devorsine.com



info@devorsine.com



06 45 92 93 55

