Assurance

CYBER RISQUES

RISQUES, ENJEUX ET SOLUTIONS

LES RISQUES :

Virus, piratage, ransomware, indisponibilité du réseau informatique, malveillance interne, risques médiatiques liés à l'utilisation des réseaux sociaux…

Les cyber risques sont devenus une réalité incontestable. Ils peuvent entraîner des répercussions graves sur votre activité et votre image

LES ENJEUX :

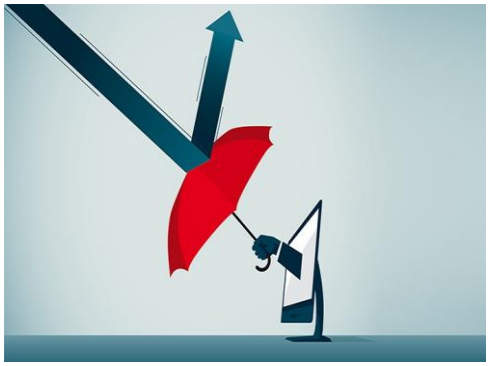
Votre organisation, votre fonctionnement
et vos échanges dépendent de vos Systèmes d'Information.

- Organisation, process, gestion des flux.
- **Hyper dépendance à l'informatique :** mails, internet, extranet…
- **Les moyens de télécommunication :** tablettes, smartphone..
- **Transformation digitale :** Cloud ou internet ou Big Data, la transformation numérique ne pourra s'opérer sans sécurité du Service Informatique
- **Data Protection & Réglementation :** Les exigences réglementaires font de la question cyber un sujet stratégique pour les dirigeants d'entreprise.

CYBERATTAQUES :

Comment chiffrer les impacts ? Le visible et l'invisible :

Données tirées du Rapport « Enjeux Cybers 2018 » du cabinet Deloitte.



LES NOUVELLES RÈGLES FACE AUX NOUVEAUX RISQUES :

RGPD (Règlement Général sur la Protection des Données)
Date d'entrée en vigueur : 25 mai 2018
• Ce nouveau règlement européen oblige les organisations à s'assurer du consentement explicite des individus quant à l'utilisation qui sera faite de leurs données

DSP 2 (Directive sur les services de paiement 2)
Date d'entrée en vigueur : 13 janvier 2018
• Cette directive européenne définit les règles concernant les nouveaux acteurs sur le marché des paiements (FinTechs).

LPM (Loi de Programmation Militaire)
Date d'entrée en vigueur des mesures de cyber-sécurité : Juillet 2016
• Cette réglementation concerne les entreprises classées « Opérateurs d'Importance Vitale » (OIV) qui sont tenues de renforcer leur niveau de sécurité (contrôles réguliers, détection des événements, alerte suite à un incident) sous peine de dispositions pénales. La directive européenne NIS, dans le même registre, est également à prendre en considération.

Programme sécurité de **SWIFT***
Date d'entrée en vigueur : Janvier 2018
• Un ensemble de standards de sécurité qui devient obligatoire pour tous les membres du réseau. Chaque membre SWIFT sera tenu de publier une auto-attestation annuelle faisant état du respect des points de contrôle obligatoires (sécurisation de l'environnement, contrôle et limite des accès, détection et réponse à un incident).

**SWIFT est une coopérative internationale détenue par ses membres et le premier fournisseur mondial de services de messagerie financière sécurisés*

AGEO RISKS

NOTRE REPONSE :

Une assurance « cyber » globale
pour vous protéger des risques numériques:

1 : Actions d'urgence

Frais et dépenses Garantis :
- Conseils juridiques
- Expert informatique
- Atteinte à la réputation
- Restauration des données
- Frais de notification
- Frais de monitoring et surveillance

2 : Les garanties des dommages subis

- Perturbation de l'exploitation
- Sanction pécuniaire prononcée par une autorité
- Cyber-extorsion
- Pertes d'exploitation
- Frais supplémentaires d'exploitation
- Fraude téléphonique: Prise en charge du coût de la surconsommation téléphonique (appel en IP sur des n° surtaxés)
- Fraude informatique: Prise en charge des pertes pécuniaires

3 : Les garanties Responsabilité Civile

- Atteintes aux données
- Atteinte à la sécurité du système informatique
- Atteinte à l'image, diffamation, calomnie…
- Manquement à l'obligation de notification

Exemples de sinistres vécus :

Panne informatique :
Une société de fabrication de pièces pour l'industrie est victime d'une panne serveur hébergeant la base de données de gestion des commandes et des stocks.
Indemnité versée: 350 000 €
Les plus gros postes
- Heures supplémentaires du personnel
- Frais supplémentaires afin d'éviter les arrêts de production client.

Erreur humaine :
Une entreprise confie une partie de ses fichiers commerciaux (clients, cartes de fidélité, prospects) à un prestataire spécialisé dans le Marketing. Une erreur humaine de ce prestataire a entrainé la fuite de dizaines de milliers de données références clients.
Indemnité versée : 140 000 euros
- Gestion de crise et assistance
- Conseil Juridique
- Frais d'investigations
- Frais de notification et centre d'appels

En savoir plus ?
Contactez Olivier BOULARD / Associé RISKS
olivier.boulard@ageo.fr
01.42.33.57.34
06.95.81.01.26
AGEO RISKS