



L'ASSURANCE BY DIAGERIS :
UNE OFFRE D'ACTION COLLABORATIVE

Aborder ce sujet demande une **DÉMARCHE STRATÉGIQUE GLOBALE** qui allie prestations de services et assurance.

UNE OFFRE D'ACTION COLLABORATIVE

DÉFINITION DU SYSTÈME D'INFORMATION :

Un système d'information (SI) est un ensemble organisé de ressources (les matériels, logiciels, personnel, données et procédures) qui permet de collecter, regrouper, classer, traiter et diffuser de l'information dans un environnement donné.

Le système d'information appréhende l'ensemble des éléments suivants :

- » Le système informatique
- » La gestion des données métiers, y compris celles confidentielles confiées par des tiers, voire les données secrètes (fruit de la R&D)
- » La gestion des données personnelles
- » Le système télécom
- » La gestion des documents papiers
- » L'organisation
- » Les locaux abritant les infrastructures informatiques
- » Les dirigeants
- » Le personnel, y compris nomade, voire nomade à l'international
- » L'image de l'entreprise

LE S.I. PEUT ÊTRE CONSIDÉRÉ COMME UN ACTIF IMMATÉRIEL DONT L'ALTÉRATION, AFFECTERA DIRECTEMENT L'ACTIVITÉ DE L'ENTREPRISE.

Aborder ce sujet demande une **DÉMARCHE STRATÉGIQUE GLOBALE** qui allie prestations de services et assurance.

UNE OFFRE D'ACTION COLLABORATIVE

QUELS SONT LES ÉVÈNEMENTS QUI PEUVENT AFFECTER LE SERVICE HABITUELLEMENT RENDU PAR LE S.I.?

Reprise de l'inventaire défini par l'AMRAE/CESIN (Club des Experts de la Sécurité de l'Informatique et du Numérique)

- » R1 > Dénis de services
- » R2 > Publication d'informations malveillances ou diffamatoires
- » R3 > Attaque d'une entreprise tierce par un pirate, via le S.I. d'une entreprise
- » R4 > Vol de données dans l'entreprise par un pirate (données appartenant à des tiers et/ou à l'entreprise)
- » R5 > Vol de données valorisables
- » R6 > Fraude
- » R7 > Indisponibilité du S.I. et du service fournis par l'infogérant
- » R8 > Panne du S.I.
- » R9 > Altération de la sécurité des données suite à un dommage matériel ayant affecté l'outil dans l'entreprise ou chez le prestataire infogérant
- » R10 > Grèves et émeutes mouvements populaires endommageant le SI de l'entreprise, d'un prestataire ou infogérant
- » R11 > Erreur de l'entreprise générant la compromission de la sécurité des données personnelles
- » R12 > Erreur de programmation de l'entreprise
- » R13 > Défaillance d'une prestation
- » R14 > Pénétration du S.I. de l'entreprise avec destruction de données
- » R15 > Atteinte à la sécurité des données suite à une intrusion dans le S.I.
- » R16 > Pénétration dans le S.I. de l'entreprise avec suspicion de détournement
- » R17 > Demande de rançon
- » R18 > Virus informatique affectant le S.I.
- » R19 > Destruction de données du fait d'un sinistre matériel
- » R20 > Fraude interne

Aborder ce sujet demande une **DÉMARCHE STRATÉGIQUE GLOBALE** qui allie prestations de services et assurance.

UNE OFFRE D'ACTION COLLABORATIVE

LISTE À LAQUELLE, ON PEUT AJOUTER DES ÉLÉMENTS COMPLÉMENTAIRES RÉPERTORIÉS PAR L'OCDE, TELS QUE :

- Le fonctionnement défectueux du réseau
- L'interruption du S.I. d'un ou plusieurs tiers, du fait de la transmission d'un malware
- L'interruption de service d'un fournisseur de services informatiques (cloud)
- L'inaccessibilité des locaux de l'entreprise

LISTE QUI PEUT ÊTRE ÉGALEMENT COMPLÉTÉE PAR DES PROBLÉMATIQUES À CARACTÈRE SOCIAL TELS QUE :

- La mise en cause prudhommale de l'entreprise, à la suite de divulgation de données à caractère personnel
- Le déclenchement d'une enquête CNIL ou Défenseur des droits

QUELLES PEUVENT ÊTRE LES CONSÉQUENCES FINANCIÈRES DE LA RÉALISATION DE CES ALÉAS ?

1/2

1- DES CONSÉQUENCES FINANCIÈRES DIRECTES :

- » Le coût de la gestion de crise (avocats, communication, e-réputation, expert...)
- » Des pertes de marchés
- » Des pénalités de retard
- » Le coût de mise en œuvre du PRA ou du PCA
- » Le coût de la reconstitution de données perdues et/ou la réparation de logiciels dégradés, dépollution du S.I.
- » Le montant du Vol d'argent: fraude, surfacturation, extorsion et demande de rançon
- » Une perte d'exploitation

2- DES CONSÉQUENCES FINANCIÈRES D'UNE MISE EN CAUSE DU FAIT :

- » De produits défectueux dus aux risques cyber
- » D'une fourniture de produits, ou de services, inadéquats du fait d'une action cyber
- » Du dysfonctionnement, du fait d'une action cyber, de travaux collectifs ou de l'utilisation d'une plateforme collaborative
- » De la transmission de virus et logiciels malveillants
- » De dommages environnementaux du fait d'une pollution liée à un incident cyber
- » De dommages aux actifs physiques liés à un incident cyber
- » D'une atteinte aux données personnelles
- » Du non respect de dispositions réglementaires

QUELLES PEUVENT ÊTRE LES CONSÉQUENCES FINANCIÈRES DE LA RÉALISATION DE CES ALÉAS ?

2/2

ET ÉGALEMENT, LES CONSÉQUENCES FINANCIÈRES D'UNE MISE EN CAUSE DES DIRIGEANTS DU FAIT :

- D'une atteinte à la sécurité
- D'un manquement aux obligations juridiques et / ou réglementaires
- D'une atteinte à l'image
- D'une perte de valorisation de l'entreprise

RÉPONSE

C'est de ce constat qu'est née une réponse originale, à cette problématique au caractère disruptif, pour guider, accompagner et défendre le chef d'entreprise face au risque de sinistre numérique au sens très large.

L'ORIGINALITÉ DE LA PROPOSITION CONSISTE À ORGANISER, AUTOUR D'UN CONTRAT D'ASSURANCE AD' HOC, LA COORDINATION DE TROIS TEMPS D'ACTIONS COLLABORATIVES, DIFFÉRENTES ET COMPLÉMENTAIRES.

TEMPS 1 : EN AMONT DESTINÉ À

- **Etablir**, sous la houlette du coordinateur Diageris, un plan d'action d'anticipation et de gestion de crise, avec une attention forte sur la continuité d'activité post sinistre,
- **Prévenir** le risque de mise en cause des dirigeants,
- **Elaborer** en conséquence les spécificités de la police d'assurance ad' hoc,
- **Procéder au suivi**, du plan d'action et de la police d'assurance ad' hoc, pour tenir compte de l'évolution des besoins de l'entreprises.

TEMPS 2 : LA COORDINATION GÉNÉRALE D'ACCOMPAGNEMENT POST SINISTRE POUR :

- **Initier immédiatement et coordonner** l'intervention d'une équipe pluridisciplinaire, mise en œuvre pour la réalisation du plan d'action prévu pour limiter les dommages et permettre la reprise d'activité « normale », et parallèlement, assurer avec les prestataires idoines, **la préservation de l'image**.
 - **Accompagner** l'entreprise à l'occasion de toute enquête menée par une autorité administrative de contrôle (CNIL ...).
-

TEMPS 3 : MISE EN ŒUVRE DE LA POLICE D'ASSURANCE AD' HOC POUR :

- **Financer** la réalisation des travaux du plan d'action prévu, y compris celui de la préservation de l'image,
- **Prendre en charges** les frais de défense, les conséquences financières de mises en cause et, les frais d'enquête menée par toute autorité administrative de contrôle,
- **Indemniser le montant** d'une éventuelle perte d'exploitation avérée.



DIAGNOSTIC ET GESTIONS DES RISQUES : ARCHITECTE EN SOLUTIONS D'ASSURANCE

infos@diageris.com - 06 03 69 60 66 - 22 Rue Germain 69006 LYON

*RCS Lyon : 442 735 478 - Orias : 07 004 767 - Garantie financière et assurance responsabilité civile professionnelle
conformes aux dispositions des Articles L512-6 et L512-7 du Code des assurances*