

ONLY MED

LE RGPD EN PRATIQUE POUR LES ENTREPRISES DE SANTÉ

LES CYBERATTAQUES ET LA SANTÉ

Les Echos.fr

LES ECHOS: Tapez votre recherche

NUMÉRIQUE & INFORMATIQUE ENERGIE & ENVIRONNEMENT MATÉRIAUX & CHIMIE

Cyberattaques

LEGALIS L'ACTUALITÉ DU DROIT DES NOUVELLES TECHNOLOGIES
2698 DÉCISIONS EN LIGNE

ACTUALITÉS JURISPRUDENCES LEGALTECH LES AVOCATS DU NET RECHERCHER OK

Newsletter Legalis
Adresse email
S'abonner

Jurisprudence / Thématique
Base de données
Contenus illicites
Diffamation
Droit d'auteur
E-commerce
Logiciel

Actualités

MARDI 12 SEPTEMBRE 2017

Traitement et hébergement illicite de données de santé

Un médecin hospitalier qui avait procédé à un traitement automatisé de données médicales sans l'autorisation de la Cnil a été condamné à une peine de 5 000 € d'amende, par un **jugement** définitif du TGI de Marseille du 7 juin 2017. Le directeur des systèmes d'information et de l'organisation de l'hôpital en cause qui avait une délégation de signature, qui constituait une réelle délégation de pouvoir, a été relaxé car il n'avait pas une réelle connaissance de l'externalisation effective des données médicales et de leur hébergement chez un prestataire non agréé. Quant à ce dernier, il a été relaxé de l'infraction relative à l'absence d'agrément pour l'hébergement de données de santé, car aucun texte ne sanctionne le fait de faire héberger ces informations par un tiers non agréé. Comme il s'agit de données très sensibles, l'article L. 1111-8 du code de la santé publique impose en effet aux hébergeurs de données de santé le respect d'un

DIRECT TV DIRECT RADIO EMAIL

5

éditeur
ances
S
stre
ncipaux
quants
bles et

çais sont-
lant

eurs infectés...

.pdf ^

LE SAVEZ VOUS ?

- Quel pourcentage des attaques, en 2016, a touché des organismes liés à la santé ?

15 %

2^{ème} secteur le plus touché après les organismes financiers (23%)

- Quel pourcentage des attaques implique le « crime organisé » ?

51 %

- Quel pourcentage des attaques implique du piratage

62 %

- Qui est à l'abris d'une telle attaque ?

0 %

LES PRINCIPALES FAILLES EN SANTÉ

Dans le secteur de la Santé, **81 % des failles** sont regroupés en **3 causes majeures** (sur 10) :

1. Mauvais usage par le **personnel interne** (malveillant ou non)
2. **Erreurs diverses** conduisant à une perte de données

dans 76 % des cas, c'est votre client qui vous l'apprend !

3. **Vol et pertes physiques**

passé de la 1^{ère} à la 3^{ème} cause entre 2016 et 2017

SÉCURITÉ DES DONNÉES, CE QUI CHANGE AVEC LE RGPD

- Des données particulièrement sensibles
- Des clients BtoB de plus en plus exigeants
- Obligation de transparence -> notification CNIL et individuelle

BANCAIRES

DE SANTÉ

CONFIDENTIELLES

DEMANDES CONTRACTUELLES
D'ASSURANCE CYBER

PLUS DE PUBLICITÉ

ONLYNNOV

NOUS ASSURONS LES FRENCHTECH

Nous avons créé une gamme de produits
et services sur mesure pour les
entreprises innovantes:

ONLY

MED

ONLY

NUM

ONLY

IOT

ONLYNNOV

ONLY
MED

DISPOSITIFS MEDICAUX
MEDTECH
HEALTH IT
BIOTECHNOLOGIES
LABORATOIRES PHARMACEUTIQUES



TROIS SITUATIONS DE RISQUE DISTINCTES

Logiciels de santé

La Responsabilité Civile Professionnelle et la gestion des données personnelles de santé sont indissociables.

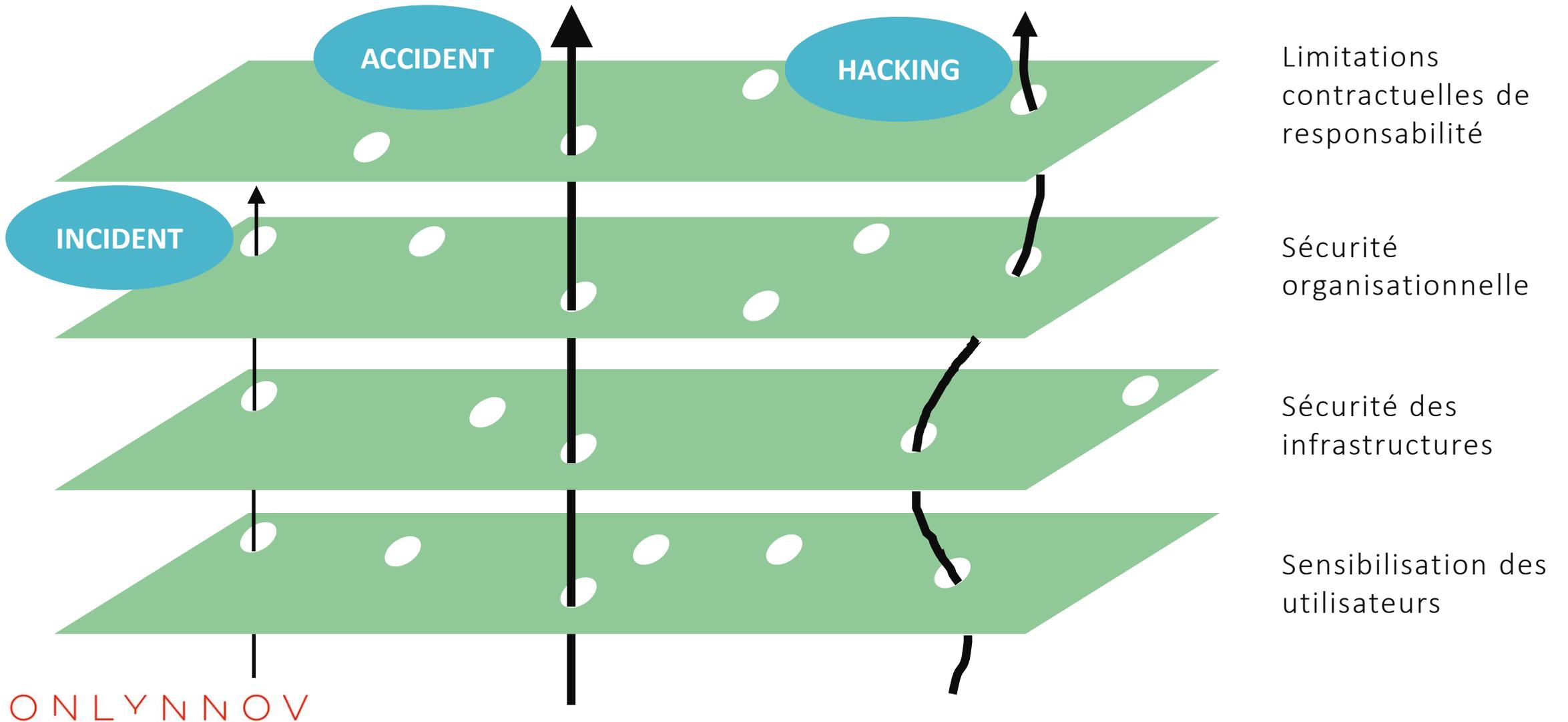
Dispositifs connectés de santé

La Responsabilité Civile Professionnelle / Produits et la gestion des données personnelles de santé sont parfois indissociables, mais pas toujours.

Autres produits de santé (DM, Pharma, ...)

La sécurité des données personnelles de santé est un sujet bien distinct du produit en lui même.

RISQUES RÉSIDUELS



Limitations contractuelles de responsabilité

Sécurité organisationnelle

Sécurité des infrastructures

Sensibilisation des utilisateurs

IMPRÉVISIBLE : LE FACTEUR HUMAIN

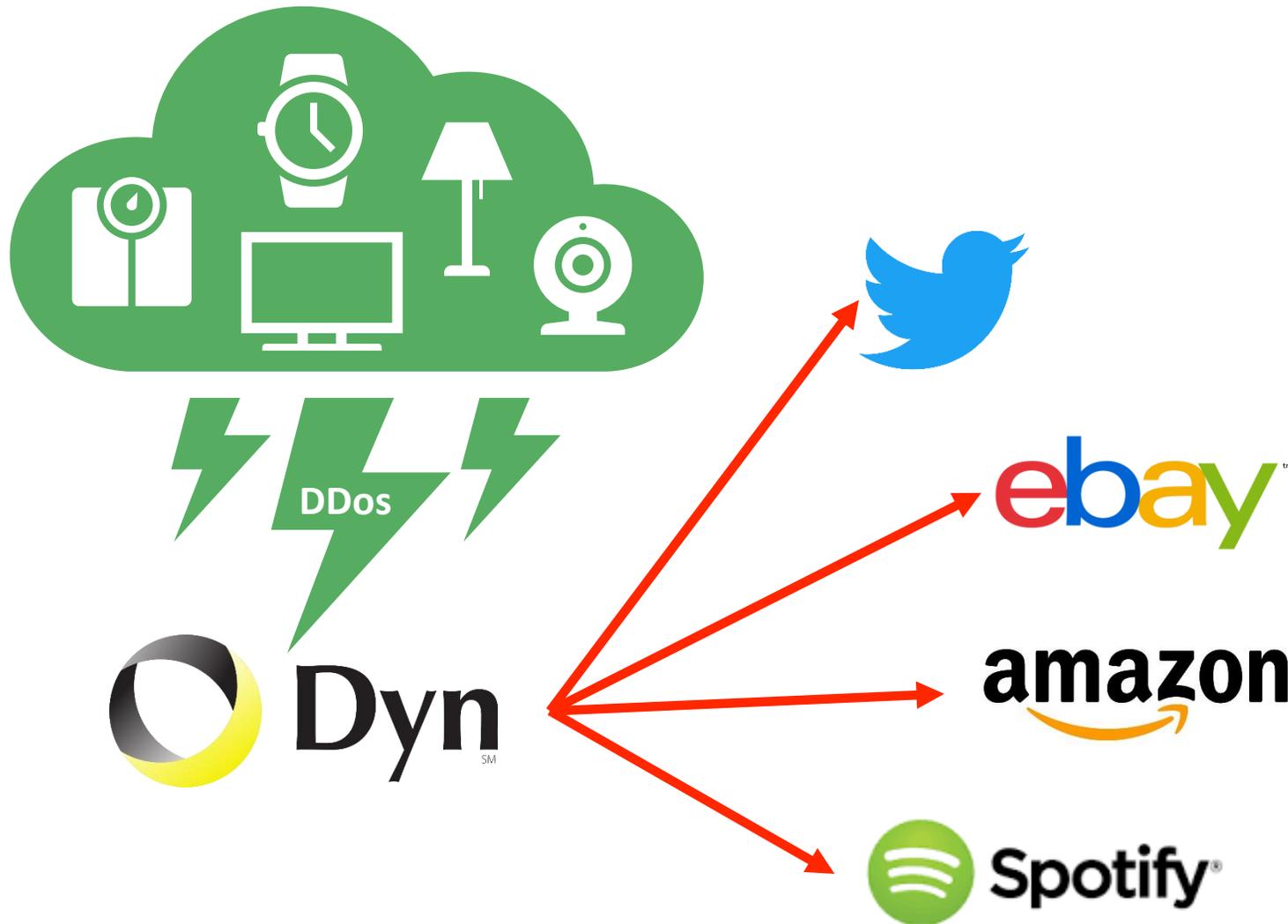
Exemple d'un sinistre réel

Une chaîne de prêt-à-porter confie une partie de ses fichiers commerciaux (clients, cartes de fidélité, prospects) à un prestataire spécialisé dans le marketing. Une erreur humaine chez ce prestataire entraîne la fuite de dizaines de milliers de références clients.

Impacts financiers

- Indemnité versée de 160 000 €
- Gestion de crise et assistance
- Conseil juridique
- Frais d'investigations
- Frais de notifications et centre d'appels

DYN : UN RISQUE HORS DE CONTRÔLE



Affaire DYN : un hacker utilise le logiciel Botnet « MIRAI » pour prendre le contrôle d'objets connectés du quotidien. Il dirige une attaque d'une ampleur exceptionnelle contre un hébergeur de serveurs DNS.

DYN : QUE DISENT LES EXPERTS ?

“ Ces attaques, en particulier avec l'essor d'objets connectés non sécurisés, vont continuer à harceler nos organisations. Malheureusement, ce que nous voyons n'est que le début en termes de botnets à grande échelle et de dommages disproportionnés. ”

Ben Johnson, ancien spécialiste en cybersécurité pour la NSA (à propos de l'affaire Dyn)

ASSURANCES CYBER, À QUOI ÇA SERT ?

Un large choix de garanties en cas d'acte malveillant, d'erreur humaine, de panne :

PRÉJUDICE DIRECT

Responsabilité Civile

- Préjudices subits par vos clients
- Préjudices subits par autres tiers

Attention à la notion de Responsabilité Civile dans les assurances RC classique !

Dommmages immatériels

- Frais supplémentaire d'exploitation
- Frais de reconstitution de données
- Pertes d'exploitation

Frais d'assistance à incident

- Cout d'investigation
- Frais de monitoring
- Frais de négociation avec CNIL ou équivalent
- Frais de notification

Autres pertes financières

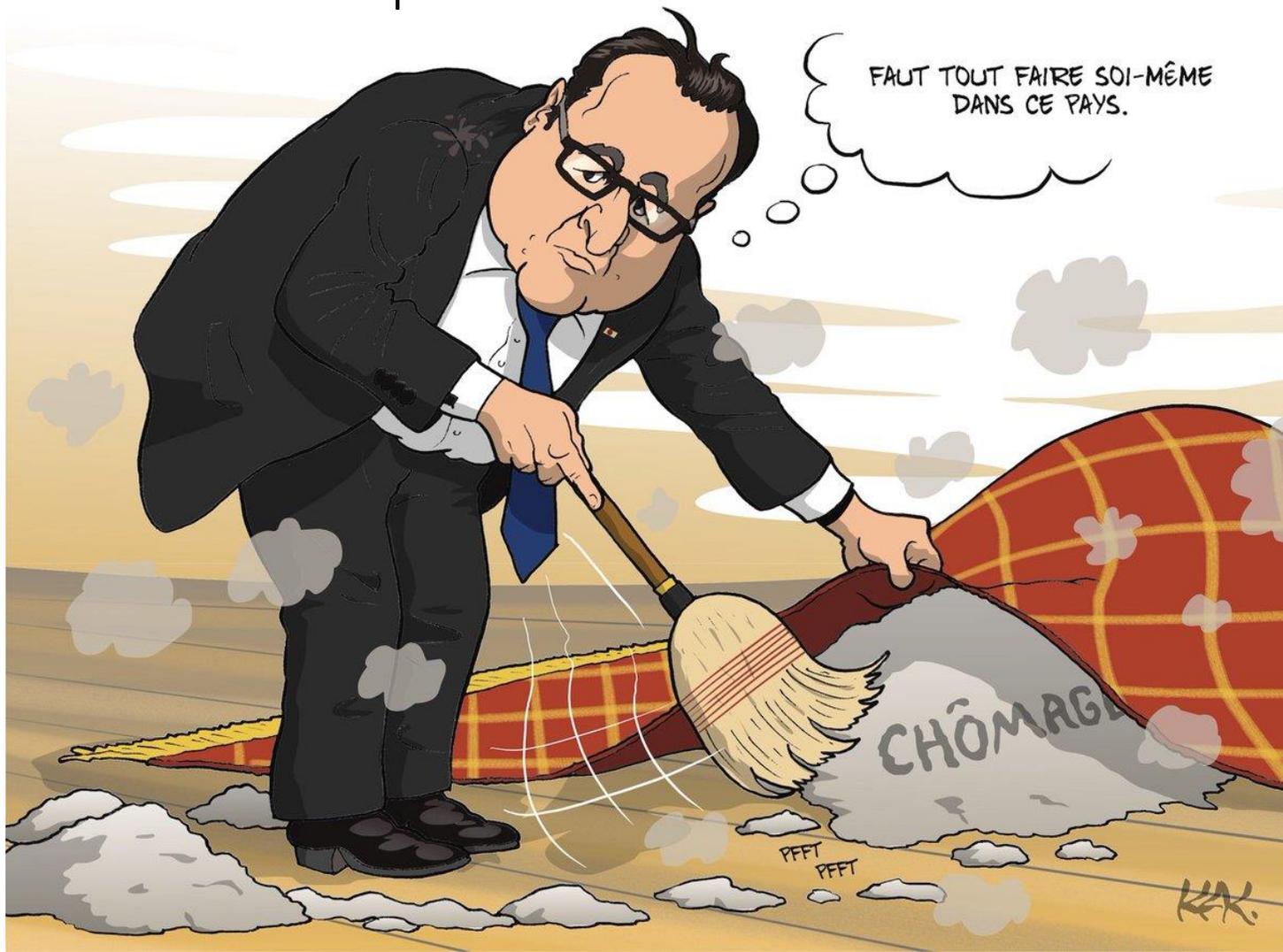
- Cyber extorsion (rançon, négo, ...)
- Sanctions réglementaires
- Pénalités PCI-DSS

AUTRES FRAIS

NE SOUS-ESTIMEZ PAS L'ASSURANCE

Quelles sont les entreprises innovantes les plus mal assurées pour leurs risques métiers ?

Les éditeurs de logiciels et les fabricants d'objets connectés de santé



HIT & IOT – MAL COMPRIS PAR LES ASSUREURS

Risques spécifiques aux Logiciels

- Engagements de résultat (SLA)
- Hébergement sous traité (SaaS)
- Gestion de projets (intégration)
- Propriété intellectuelle
- Hacking
- Préjudices immatériels pures

**Assurance RC Professionnelle
Spéciale pour le Numérique**

Risques spécifiques aux DM

- Dommages corporels sur patients
- **Obligation légale d'assurance**

**Assurance RC Produits
spéciale pour les DM**

Aucune assurance standard adaptée à la double spécificité du HIT / IOT

HIT & IOT – MAL COMPRIS PAR LES ASSUREURS

Risques spécifiques aux Logiciels

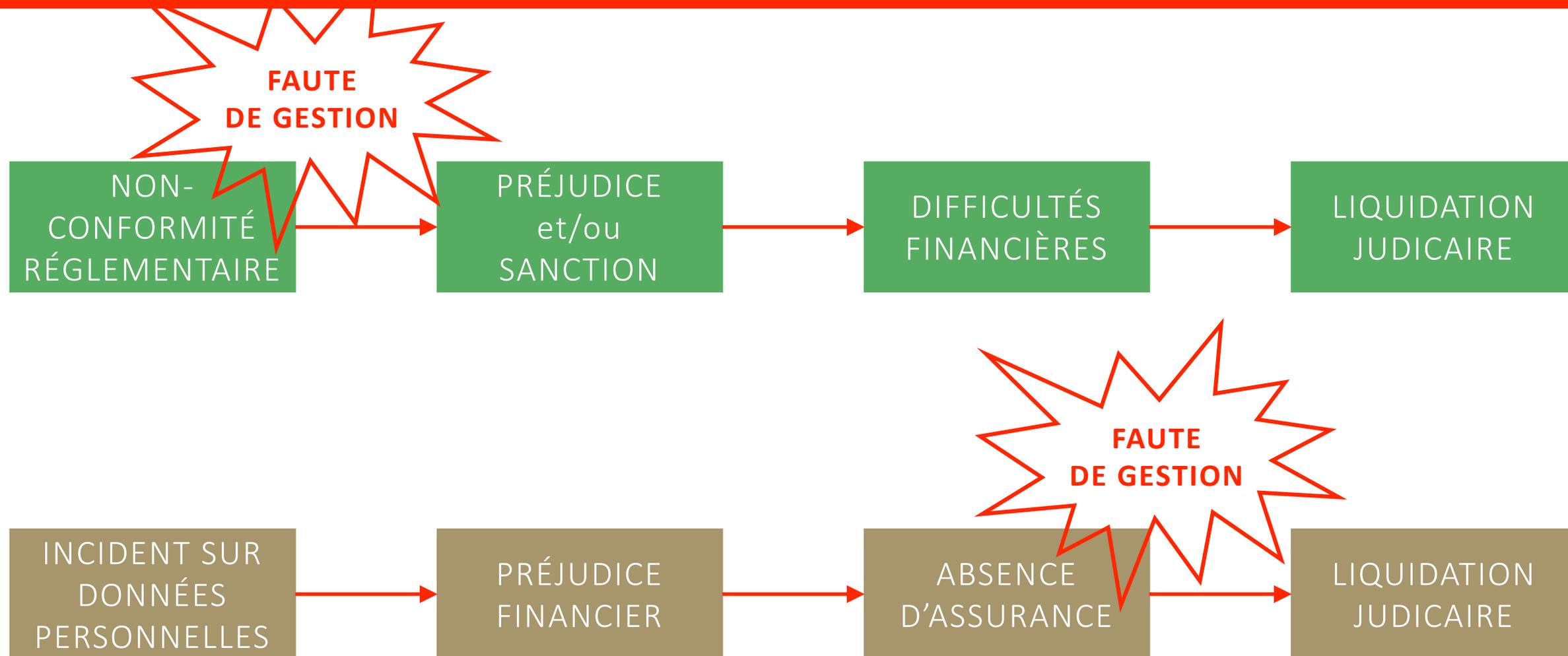
- Engagements de résultat (SLA)
- Hébergement sous traité (SaaS)
- Gestion de projets (intégration)
- Propriété intellectuelle
- Hacking
- Préjudices immatériels pures

Risques spécifiques aux DM

- Dommages corporels sur patients
- **Obligation légale d'assurance**

Assurance RC Professionnelle/Produits spécifiquement adaptée aux logiciels de santé et IOT de santé, y compris pour les risques liés à la sécurité des données personnelles de santé et les conséquences de hacking

AUTRES RISQUES POUR LES DIRIGEANTS



AUTRES RISQUES POUR LES DIRIGEANTS



EN CAS DE LIQUIDATION, LE MANDATAIRE JUDICIAIRE POURSUIT LE DIRIGEANT POUR FAUTE DE GESTION DANS ENVIRON 30% DES CAS

LES ACTIONNAIRES, LES SALARIÉS, LES TIERS PEUVENT AUSSI POURSUIVRE LE DIRIGEANT POUR FAUTE DE GESTION, MÊME SANS LIQUIDATION

RESPONSABILITÉ PÉNALE pour les DPO, RSSI, DSI, dirigeants

RECOMMANDATION DE PLAN D' ACTIONS

1

AUDITER SON ASSURANCE
RC PROFESSIONNELLE

2

PRENDRE UNE ASSURANCE
POUR LES RISQUES CYBER

3

AUDITER / SOUSCRIRE UNE ASSURANCE
RESPONSABILITÉ DES DIRIGEANTS

4

LE VALORISER
AUPRÈS DE
VOS CLIENTS

ONLYNNOV

NOUS ASSURONS LES FRENCHTECH

EN FRANCE
ET À L'INTERNATIONAL

[ONLYNNOV.COM](https://onlynno.com)

AVERTISSEMENT

Ce document est la propriété d'**ONLYNNOV** et de son auteur M **Guillaume SANTIAGO**. Vous êtes autorisé à copier le présent fichier et à le diffuser , non modifié, par tout moyen et pour toute finalité, à condition de reproduire ou citer les noms et qualités de l'auteur et de sa société. Les droits ainsi concédés valent pour le monde et la durée de protection par le droit d'auteur.

Aucune forme d'exploitation commerciale de ce document n'est autorisée, qu'elle soit directe ou indirecte. À ce titre, il est notamment strictement interdit de partager ce document avec tout assureur et/ou intermédiaire en assurance.

En cas de doute : nous contacter (info@onlynnov.com)