ONLY

MED

LE RGPD EN PRATIQUE POUR LES ENTREPRISES DE SANTÉ

Jeudi 11 janvier 2018– MEDICALPS - Grenoble

ONLYNNOV

LES CYBERATTAQUES ET LA SANTÉ

LE SAVEZ VOUS ?

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

15 %

2ème 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 %

Source : rapport VERIZON 2017

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 1ère à la 3ème cause entre 2016 et 2017

Source : rapports VERIZON 2016 et 2017

SÉCURITÉ DES DONNÉES, CE QUI CHANGE AVEC LE RGPD

- Des données particulièrement sensibles

BANCAIRES

DE SANTÉ

CONFIDENTIELLES

- Des clients BtoB de plus en plus exigeants

DEMANDES CONTRACTUELLES D'ASSURANCE CYBER

- Obligation de transparence -> notification CNIL et individuelle

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

ASTON medical Orthopaedic Implants

NORAKER INNOVATIVE BIOMATERIALS

MedicalGroup Corp EN ISO 13485 Implant Contract Manufacturer

PIXYL

ASPIDE MEDICAL

DEEPLINK MEDICAL

SEM science et médecine FABRICANT FRANÇAIS

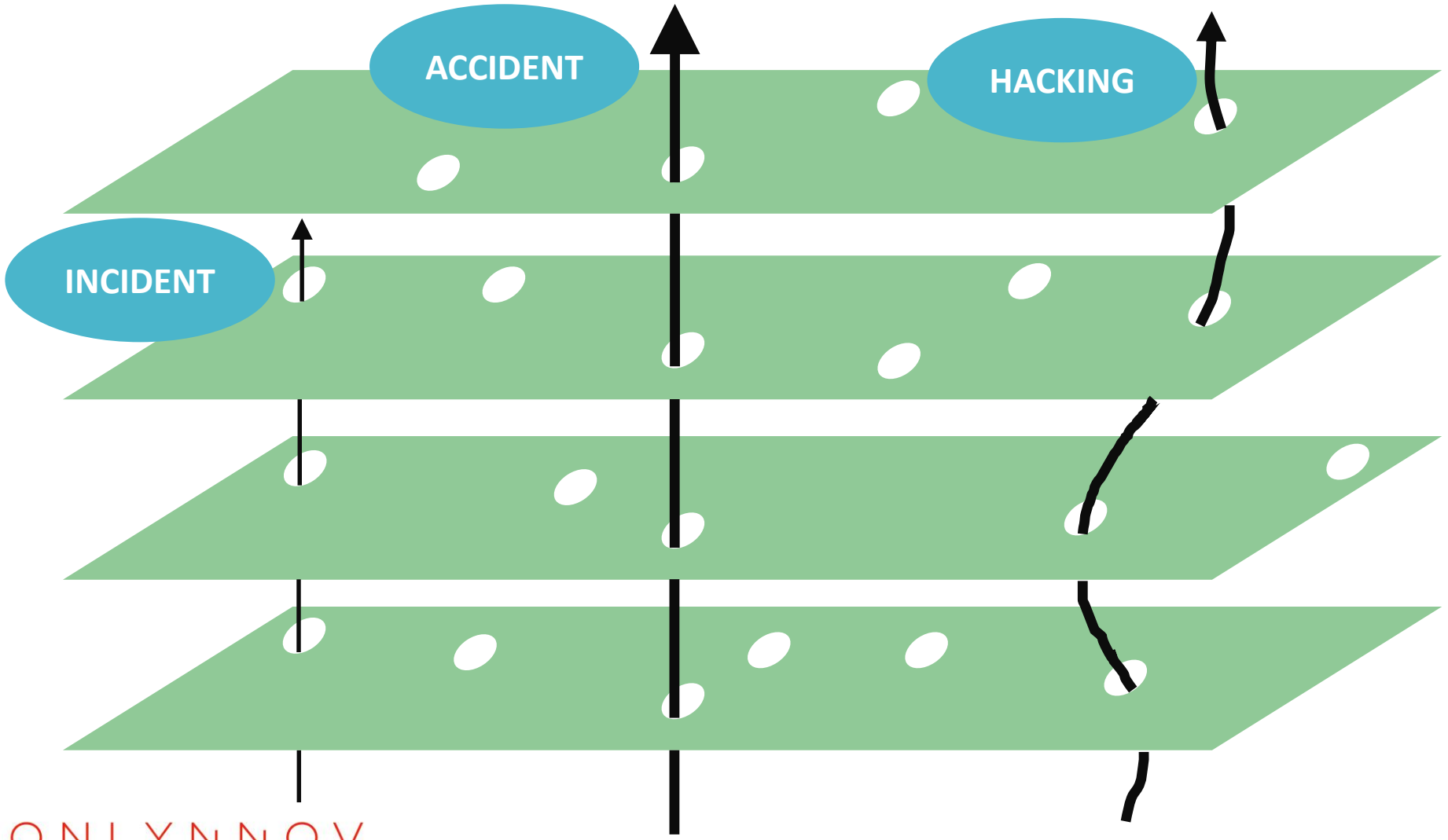
endodiag

TRANSCURE BIOSERVICES

TROIS SITUATIONS DE RISQUE DISTINCTES

Logiciels de santé	Dispositifs connectés de santé	Autres produits de santé (DM, Pharma, …)
La Responsabilité Civile Professionnelle et la gestion des données personnelles de santé sont indissociables.	La Responsabilité Civile Professionnelle / Produits et la gestion des données personnelles de santé sont parfois indissociables, mais pas toujours.	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

ONLYNNOV

IMPRÉVISIBLE : LE FACTEUR HUMAIN

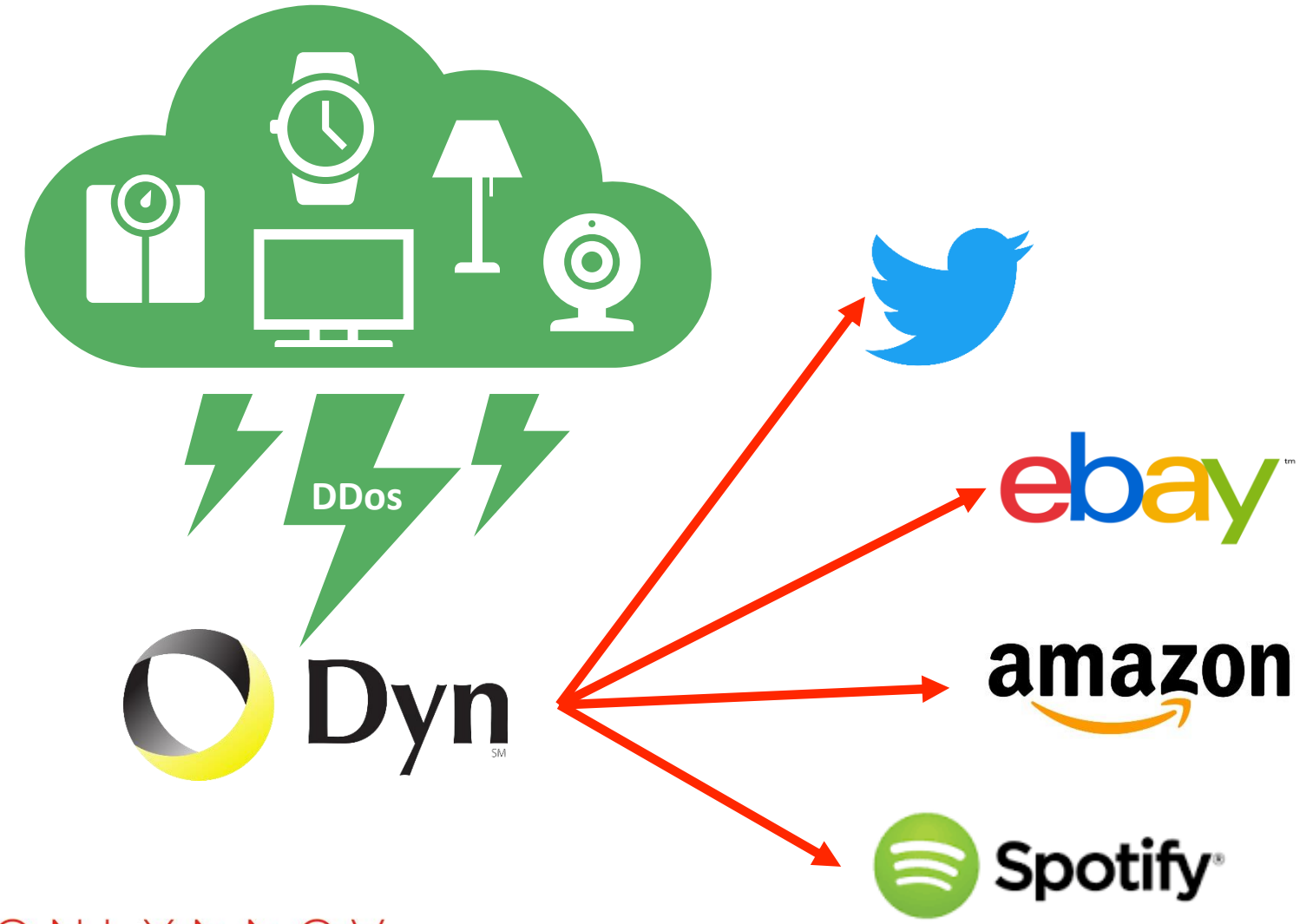
Exemple d'un sinistre réel

Une chaine 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 entraine 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 !

Dommages immatériels

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

AUTRES FRAIS

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

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

ONLYNNOV

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 Spéciale pour le Numérique

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

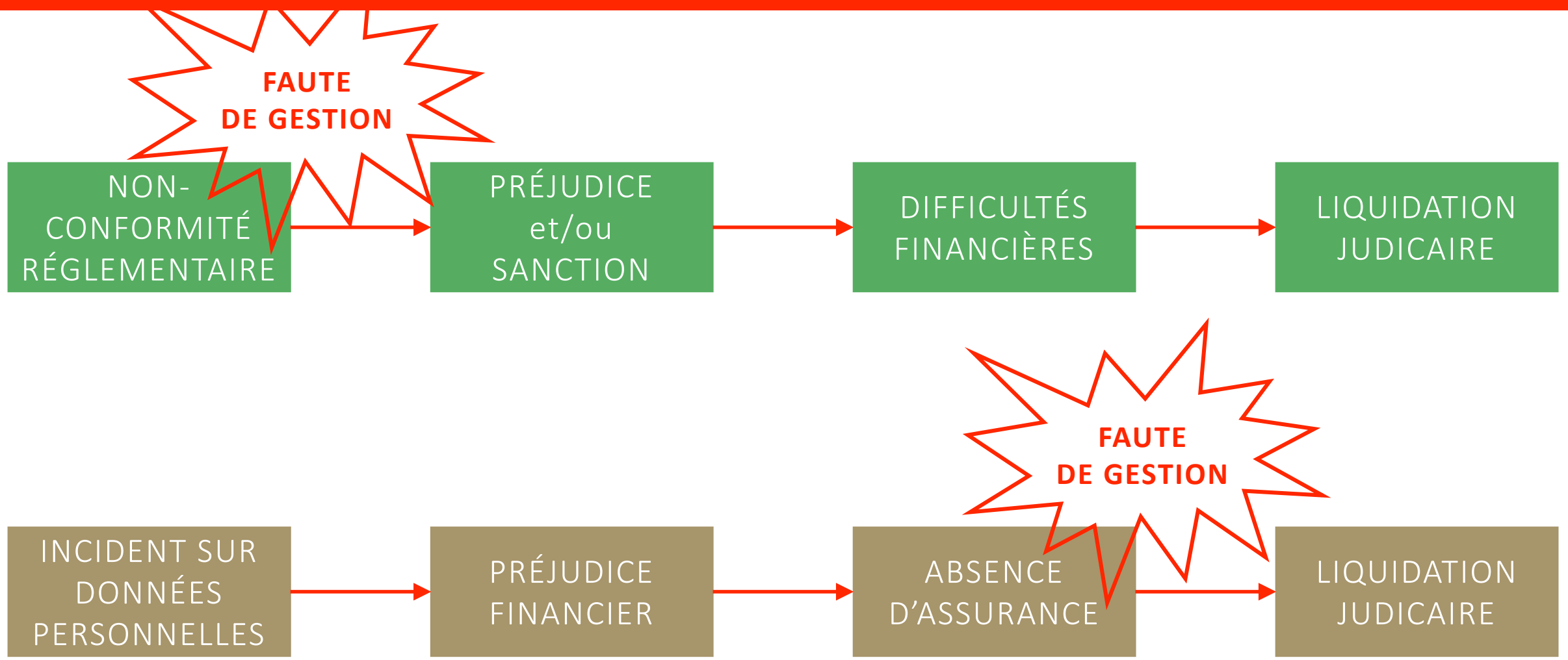
- Engagements de résultat (SLA)
- Hébergement sous traité (SaaS)
- Gestion de projets (intégration)
- Propriété intellectuelle
- Hacking
- Préjudices immatériels pures

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

AVERTISSEMENT