Les établissements sont tenus de protéger la confidentialité des informations qu'ils détiennent sur les personnes qu'ils accueillent. Quels sont les risques d'une cyber attaque ? Pourquoi s'assurer ? Comment s'assurer ?

Les établissements de soins qui s'interrogent sur le risque Cyber réalisent très rapidement qu'ils sont vulnérables et que les enjeux, tels que la confidentialité des données médicales et la sécurité des systèmes informatiques, n'ont pas été suffisamment évalués ou ne sont plus pertinents face à la menace cyber actuelle. Cette prise de conscience de l'exposition au risque cyber les oblige à arbitrer rationnellement entre les dépenses de prévention et de protection et celles du transfert du risque vers un assureur.

Seule une garantie spécifique pourra protéger l'établissement de soins contre les pertes liées à une attaque cyber, car cette garantie est généralement exclus des contrats Responsabilité Civile Professionnelle et Dommages aux Biens dont ils bénéficient.

Les pertes causées par le risque Cyber peuvent être importantes, en mettant en cause la pérennité de l'établissement de soins et en écornant son image publique.

L'assurance est là pour couvrir l'aléa que la prévention n'a pas permis d'éviter.

1) La définition du risque

Une cyber attaque est un acte de malveillance informatique qui peut prendre de multiples formes :

- virus,
- piratage informatique,
- espionnage,
- vol de données,
- malveillance d'un employé,
- tentative de cyber extorsion de fonds,
- espionnage économique ou industriel.

Une cyber attaque engendre toujours d'importantes répercussions sur l'activité de l'entreprise concernée. Ces répercussions seront d'autant plus graves qu'elles concernent un établissement de soins, détenteur de données personnelles très sensibles puisqu'elles concernent l'état de santé des patients.

2) la réglementation applicable

" Les établissements sont tenus de protéger la confidentialité des informations qu'ils détiennent sur les personnes qu'ils accueillent " (Article L1112-1 Code de Santé Publique).
Les établissements de soins ne peuvent donc se soustraire à la plus grande vigilance concernant la conservation et la sécurité des données qu'ils recueillent, notamment auprès des patients (numéro de sécurité sociale, mutuelle, informations sur l'état de santé, mais aussi références bancaires...).
Le renforcement législatif et réglementaire applicable depuis le 5 Mai 2018 grâce à l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) renforce encore la responsabilité des établissements de soins sur ce sujet.
Le Règlement Général sur la Protection des Données impose donc de nouvelles obligations, applicables aux établissements de soins, qui les contraignent à mettre en œuvre de nouvelles procédures, en particulier des notifications à toutes les personnes dont les données ont été affectées ou sont supposées avoir été affectées par l'attaque Cyber.

- **Les obligations :**
  - Notification de toute violation constatée ou supposée à la CNIL dans un délai de 72h.
  - Notification individuelle à chaque personne concernée.
  - Prise de toutes mesures nécessaires pour remédier à l'incident.
- **Les sanctions :**

Il peut être prononcé une condamnation dont le montant peut atteindre 4 % du Chiffre d'affaires annuel en cas de manquement à l'obligation de sécurisation des données.

En outre, le coût des notifications à chacune des personnes concernées (ou à toutes les personnes si l'identification des personnes visées ne peut être faite) s'élève à environ 100 € / notification.

A titre d'exemple, une violation impactant un fichier contenant 10 000 données de patients, représente un coût de 1 000 000 €, sans tenir compte du coût humain pour adresser un tel volume de courrier, et de l'impact médiatique certain d'une attaque.

3) Les préjudices liés à une attaque cyber

Les attaques cyber sont devenues une réalité incontestable, quel que soit le secteur d'activité.
L'informatisation grandissante dans le domaine de la santé avec la dématérialisation des dossiers des patients, par exemple, et l'utilisation de nouvelles technologies, expose davantage les établissements de santé aux attaques des systèmes informatiques.

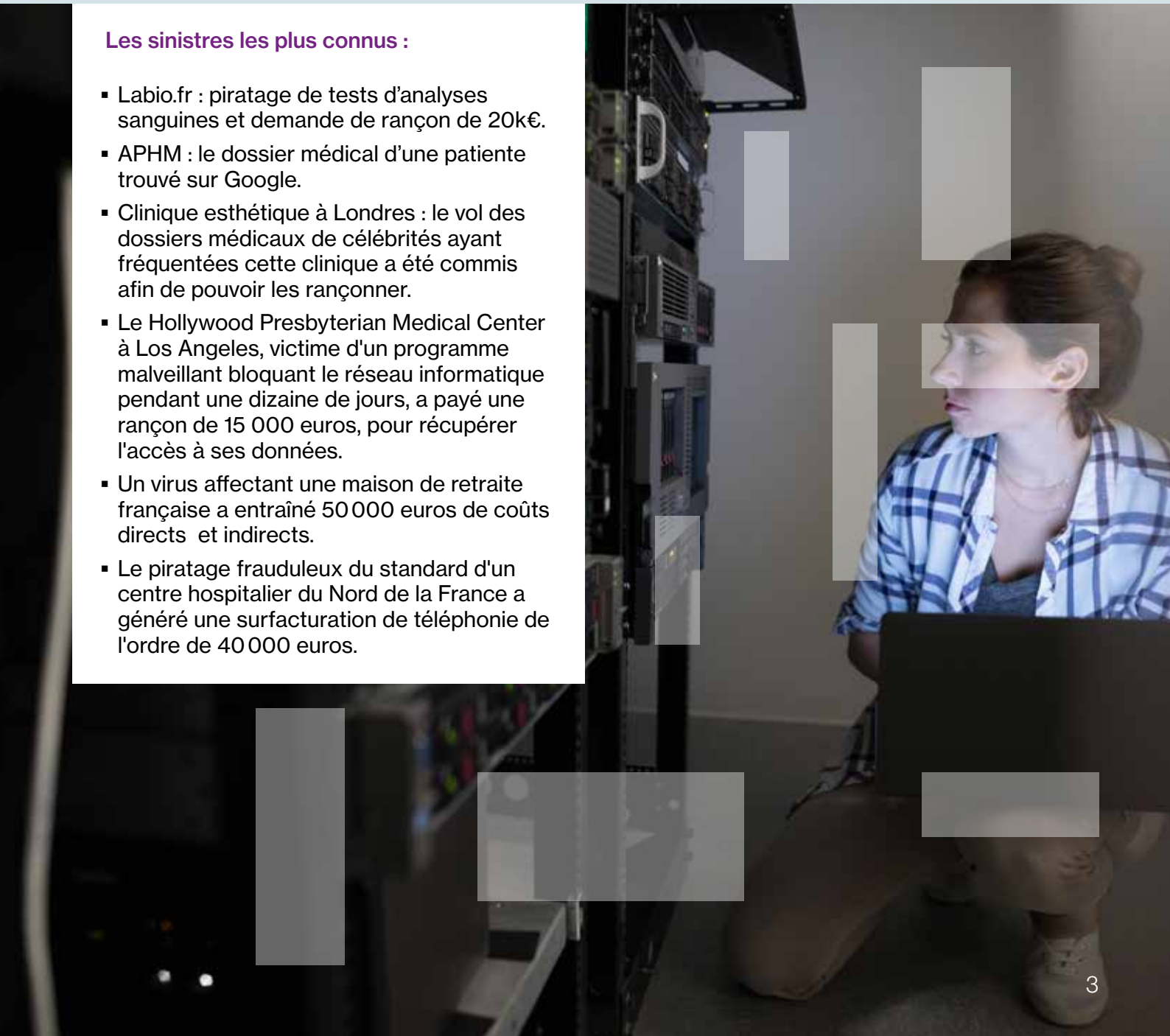
Quelques exemples de préjudices consécutifs à une cyber attaque :

- Indisponibilité, altération, destruction ou perte des données stockées au sein de l'établissement ou chez un tiers.
- Atteinte aux informations impactant le chiffre d'affaires de l'établissement de soins.
- Des données à caractère personnel peuvent être volées (données personnelles des patients, codes d'accès, coordonnées bancaires, dossiers médicaux...).

Les établissements de soins sont particulièrement vulnérables en raison des données qu'ils collectent. En effet, les données médicales sont les plus prisées des hackeurs car ce sont des données extrêmement sensibles.
D'ailleurs, 90 % des attaques ransomware survenues au deuxième trimestre 2016 ont visé des établissements de santé dans le monde (article de la société spécialisée Lexsi).

Les sinistres les plus connus :

- Labio.fr : piratage de tests d'analyses sanguines et demande de rançon de 20k€.
- APHM : le dossier médical d'une patiente trouvé sur Google.
- Clinique esthétique à Londres : le vol des dossiers médicaux de célébrités ayant fréquentées cette clinique a été commis afin de pouvoir les rançonner.
- Le Hollywood Presbyterian Medical Center à Los Angeles, victime d'un programme malveillant bloquant le réseau informatique pendant une dizaine de jours, a payé une rançon de 15 000 euros, pour récupérer l'accès à ses données.
- Un virus affectant une maison de retraite française a entraîné 50 000 euros de coûts directs et indirects.
- Le piratage frauduleux du standard d'un centre hospitalier du Nord de la France a généré une surfacturation de téléphonie de l'ordre de 40 000 euros.



Ce qu'il faut retenir :

Si l'assurance Cyber n'est pas obligatoire, elle est devenue, au regard des risques grandissant qui touchent les établissements de santé, une garantie essentielle.

Les garanties cyber doivent assurer :

- la protection de l'activité de l'entreprise (pertes exploitation et surcoûts de fonctionnement)
- les atteintes à la sécurité informatique et aux données personnelles (frais de défense, dommages et intérêts réclamés par tiers, amendes et sanctions financières réclamées par les autorités compétentes)
- l'assistance à la "gestion de crise" qui permet d'assurer la continuité de l'activité de l'entreprise et d'éviter une crise de réputation (expertise informatique, expert en gestion de crise, avocat spécialisé, ...).

Un volet " fraude " peut compléter les garanties cyber afin de permettre la prise en charge des dommages causés par une attaque cyber frauduleuse.

A propos de Willis Towers Watson

Willis Towers Watson (NASDAQ : WLTW) est une entreprise internationale de conseil, de courtage et de solutions logicielles qui accompagne ses clients à travers le monde afin de transformer le risque en opportunité de croissance.
Willis Towers Watson compte 45 000 salariés présents dans plus de 140 pays et marchés. Nous concevons et fournissons des solutions qui gèrent le risque, accompagnent les talents et optimisent les profits afin de protéger et de renforcer les organisations et les personnes. Notre vision, unique sur le marché, nous permet d'identifier les enjeux clés au croisement entre talents, actifs et idées : la formule qui stimule la performance de l'entreprise. Ensemble, nous libérons les potentiels.
Pour en savoir plus : www.willistowerswatson.com

GRAS SAVOYE, Société de courtage d'assurance et de réassurance
Siège Social : Immeuble Quai 33, 33/34 quai de Dion-Bouton, CS 70001, 92814 Puteaux Cedex.
Tél : 01 41 43 50 00. Télécopie : 01 41 43 55 55. http://www.grassavoye.com.
Société par actions simplifiée au capital de 1 432 600 euros. 311 248 637 RCS Nanterre.
N° FR 61 311 248 637. Intermédiaire immatriculé à l'ORIAS sous le n° 07 001 707 (http://www.orias.fr).
Gras Savoye est soumis au contrôle de l'ACPR (Autorité de Contrôle Prudentiel et de Résolution)
4 Place de Budapest 75436 Paris Cedex 9.

18/04/19

willistowerswatson.com

GRAS SAVOYE
Willis Towers Watson