

Management du risque cyber



Le management des risques



Soutenir la continuité de votre activité, sécuriser les parcours de soin et réduire le coût du risque sont les principaux objectifs du management des risques chez Relyens.

Notre métier est de comprendre et d'agir sur les risques auxquels vous êtes exposés, qu'ils soient associés :

- aux soins,
- à la technologie, dont Cyber,
- ou encore à vos équipes.

Notre expérience de plusieurs décennies nous a permis d'élaborer une **approche globale** pour répondre à **vos enjeux de sécurisation** de vos missions.

Piloter

Prévenir

Assurer

La cybercriminalité est un nouveau facteur de rupture de la sécurisation des soins

La sécurité des patients et la continuité des soins sont aujourd'hui mises en danger par la montée en puissance d'activités de cybercriminalité.

L'usage grandissant de la technologie rend les établissements plus vulnérables par :

- L'exposition à de nombreux dysfonctionnements internes (pannes, bugs) démultipliés par le nombre de dispositifs connectés.
- L'exposition aux tentatives d'extorsions (ransomwares) du fait de leur dépendance à la donnée numérique et aux dispositifs connectés.

733

événements
déclarés en 2022
soit + de 2 incidents/jour *

* Source Cert Santé 2023

Pour faire face à cette menace cyber, nous vous proposons une approche globale, en prenant en compte la maturité de chaque établissement en termes de politique de sécurité.

Piloter. Comprendre votre niveau de risque

grâce à la solution de pilotage du risque cyber



Comment ?

La solution innovante et inédite pour :

- **Quantifier le risque** de manière descriptive et prédictive et mettre en place un plan d'actions adapté
- Bénéficier de **recommandations actionnables et de solutions opérationnelles** adaptées à votre environnement pour réduire l'exposition aux risques et en limiter les impacts

Relyens s'est associé à Citalid, start-up Française spécialisée en « Cyber Threat Intelligence » (CTI)* pour codévelopper une solution unique et souveraine de pilotage des risques cyber. Celle-ci calcule de façon précise et estime en euros le risque cyber et les pertes associées aux différents scénarios d'attaque auxquels est exposé chaque établissement de santé.

*CTI : La cyber threat intelligence définit la recherche, l'analyse et la modélisation de la menace cyber

Pour quels résultats ?

- **Un pilotage complet** : de la vision stratégique jusqu'à l'approche opérationnelle.
- **Des indicateurs prédictifs** déclinés selon 2 scénarios (rançongiciels et fuite de données) :
 - le nombre de cyberattaques que votre établissement peut subir
 - La probabilité de réussite
 - Le coût financier moyen et maximum personnalisé (dont les pertes d'exploitation, frais de fonctionnement supplémentaires...)
 - La provision annuelle adaptée pour couvrir le risque
 - Des recommandations adaptées à votre contexte
- Une sélection de **solutions technologiques** de prévention adaptée à vos besoins
- **Une rationalisation et une planification des mesures** de sécurité à mettre en œuvre dans votre établissement
- **Une supervision dynamique** de vos risques en fonction de l'évolution des menaces

Toutes les données de Relyens, Ospi et Citalid sont hébergées en France. L'ensemble des communications entre les sources et les différentes solutions est entièrement chiffré. Vous êtes ainsi assuré de bénéficier d'infrastructures conformes, d'installations d'un haut niveau de sécurité et d'un cadre juridique sécurisé pour garantir la confidentialité et la sécurité maximales de vos données.

Pour faciliter l'accès, notre solution est intégrée à l'écosystème de la plateforme Ospivision de Ospi, l'outil d'analyse et de pilotage des activités des établissements de santé.

Prévenir et sécuriser

pour réduire le risque



Comment ?

Nous proposons en partenariat avec Forescout, leader mondial de la cybersécurité, une solution technologique innovante dédiée aux enjeux du monde de la santé.

Vous bénéficiez d'une :

- **Cartographie complète et catégorisation** de tous les dispositifs connectés sur le réseau de l'établissement ;
- **Identification de la surface d'exposition** : évaluation du risque pour chaque dispositif en fonction de leur proximité au patient (vulnérabilité, menace, conformité) ;
- **Analyse des flux de communication** au sein du réseau et détection des anomalies comportementales ;
- **Gouvernance du risque** : établissement de rapports IT et biomédical générés automatiquement par la solution et possibilité de personnaliser vos propres rapports.

Assurer pour limiter l'impact financier et réputationnel



Une prise en charge de l'incident : Assurance cyber

Parce que le risque zéro n'existe pas, nous vous proposons un dispositif assurantiel qui vient compléter notre démarche de réduction des risques en couvrant le risque résiduel.

L'assurance Cyber est un produit spécifiquement développé pour les acteurs de la santé :

- Elle inclut des garanties de gestion d'incident, de remise en état en cas d'atteinte aux données personnelles, et protège la responsabilité de l'établissement en cas d'atteinte à des données personnelles,
- La prise en charge des démarches de validation d'intégrité des données patients par les éditeurs respectifs avant remise en service du système d'information.

Si vous êtes adhérent UniHA, nous vous proposons une offre d'accompagnement global :

Un ensemble de solutions



pour une protection optimale :

- **Prévention** Anticiper les événements indésirables
- **Couverture du risque résiduel**
- **Assistance** Mieux maîtriser et réduire les conséquences du risque

Si vous n'êtes pas adhérent, nous co-construisons un programme sur mesure.

Accompagnement à la gestion de crise

Nous intervenons dès les premiers instants du sinistre via l'assistance et lors de la gestion de crise :

- Une prise en charge et assistance téléphonique.
- Assistance juridique pour répondre à vos questions, assurée par les juristes Relyens.
- Un accompagnement personnalisé et le suivi d'incidents par des experts informatiques et sécurité.
- Une assistance à la communication de crise en cas d'événements médiatiques pouvant nuire à la réputation de l'établissement.
- En cas de cyberattaque, une assistance 24x7, assurée par une équipe d'experts multidisciplinaire.

**Une approche vertueuse de management du risque lié aux soins,
AVANT, PENDANT et APRÈS l'incident :**

Piloter

Prévenir

Assurer

Un conseil, une information ?

Contactez nos experts au 04 72 75 20 00
client.adp@relyens.eu

relyens.eu



Relyens Mutual Insurance

Siège social : 18 rue Edouard Rochet - 69372 LYON Cedex 08 - FRANCE
Tél : +33 (0)4 72 75 50 25 - Société d'Assurance Mutuelle à cotisations fixes. Entreprise régie
par le code des assurances - 779 860 881 RCS Lyon. Organisme de formation professionnelle
déclaré sous le n° 82690051369 auprès du Préfet de région.
N° TVA Intracommunautaire : FR 79779860881.



GRUPE MUTUALISTE EUROPÉEN
ASSURANCE ET MANAGEMENT DES RISQUES