

# Cyber-risques.

# Attaque informatique.



# Dommmages couverts.

**simple. clair. helvetia** 

Votre assureur suisse

# Helvetia Cyber-assurance.

Une couverture complète contre les cyber-risques.



Le numérique influe sur les processus d'affaires actuels et plus aucun secteur ne saurait s'en passer. L'activité en réseau croissante qui en résulte a pour corollaire une hausse des cyber-risques auxquels votre système informatique est exposé. Pour les entreprises, se protéger contre les cyber-risques devient dès lors essentiel.

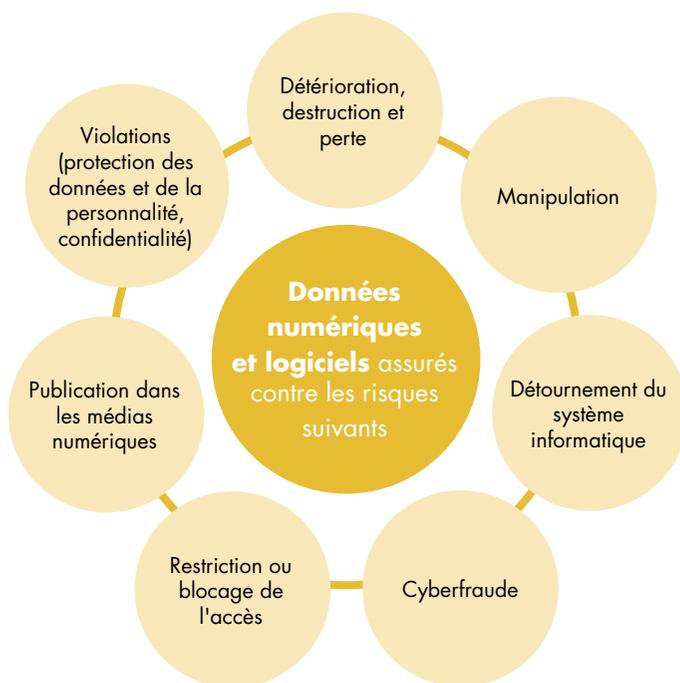
## Protection contre les conséquences de la cyber-criminalité et des causes non criminelles

Les entreprises n'ont pas d'autre choix que de protéger leurs données numériques et leurs logiciels contre la cyber-criminalité. Pourtant, quelles que soient les mesures prises, les pirates informatiques parviennent toujours à se glisser dans les failles. Ils se procurent un accès non autorisé à des données confidentielles qu'ils cryptent, détruisent ou volent, installent des logiciels malveillants ou bloquent l'accès au système informatique. Pour les entreprises, les violations de la protection des données et de la personnalité peuvent donner lieu à des litiges onéreux.

*«Les cyber-risques, comme les virus de la grippe, sont en mutation constante, si bien que même d'excellentes mesures de sécurité techniques et organisationnelles ne suffisent pas à garantir une protection complète. La cyber-assurance constitue un complément optimal pour combler ces lacunes.»*

Les cyber-risques ne sont pas forcément de nature criminelle. Il suffit souvent d'un moment d'inattention pour que des données sensibles aboutissent par mégarde dans de mauvaises mains ou disparaissent. Une brève interruption de courant ou une variation de tension peut également engendrer une perte de données. C'est pour prévenir ces risques que nous sommes là pour vous.

**Nous remboursons les dommages économiques et les frais liés aux cyber-risques suivants**



## Ces risques sont causés par

- des actes de sabotage commis par le personnel de l'entreprise
- l'exploitation d'une faille du système à caractère technique ou relative à la sécurité
- l'installation et l'exécution de logiciels malveillants
- l'utilisation de matériel non autorisé
- l'utilisation de données d'accès volées
- des attaques DoS (Denial of Service)
- une utilisation négligente par le personnel de l'entreprise
- des pannes de courte durée



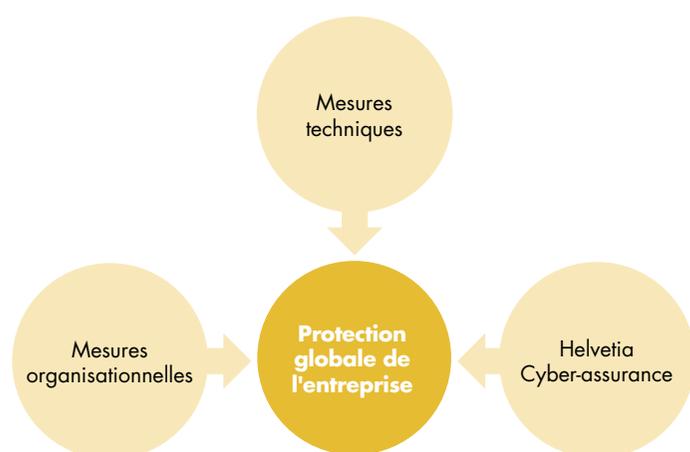
# Prévenir les risques et protéger efficacement les entreprises

## Comment vous protéger contre les cyber-risques?

Des mesures de sécurité techniques et organisationnelles permettent de réduire considérablement le risque de cyber-dommages. Instituée par la Confédération, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI publie à cet égard des recommandations pour les PME. Sur la base de ces recommandations et en coopération avec son propre réseau d'experts, Helvetia a élaboré un répertoire des mesures de sécurité dont chaque entreprise, pour se protéger, devrait s'efforcer de suivre les consignes (voir check-list page 4).

## Minimisation du risque grâce à la cyber-assurance Helvetia

Même en respectant scrupuleusement toutes les mesures de sécurité, on n'a pas la garantie d'une protection absolue contre les cyber-risques, tant ils sont multiples. La cyber-assurance Helvetia prend en charge les risques qui ne peuvent être couverts par des mesures de sécurité techniques et organisationnelles: elle constitue ainsi, pour toute entreprise, un complément idéal à la gestion des risques.



## Vos avantages en bref

- Complément important pour une gestion globale de la cybersécurité
- Couverture des coûts exceptionnels et imprévisibles
- Protection contre la perte de gain
- Couverture spéciale pour les entreprises de production utilisant le numérique (Industrie 4.0)
- Assistance en cas de violations de la protection des données et/ou de prétentions de tiers en responsabilité civile
- En cas de sinistre, accès à un réseau d'experts composé de spécialistes de la sécurité informatique et de la sécurité des données, de conseillers en communication et de conseillers juridiques
- Aide rapide et professionnelle par des experts en cas de cyberdommage (hotline cyberdommage 24h/24, 7j/7)

# Check-list

Vérifiez votre situation en matière de sécurité. Avez-vous pensé aux mesures suivantes?

- Désignation d'un-e responsable sécurité informatique**
- Gestion des autorisations**
- Directives en matière de mots de passe**
- Sensibilisation et formation du personnel à la sécurité informatique et aux cyber-risques**
- Sauvegardes quotidiennes et conservation des supports en lieu sûr**
- Mesures de protection techniques (p. ex. pare-feu, détecteur de virus, filtre anti-spam, etc.)**
- Mesures de sécurité physiques (p. ex. accès réservé aux salles de serveurs)**
- Gestion des correctifs et des mises à jour**
- Cryptage des données sensibles**
- Application des normes PCI-DSS pour les transactions par carte de crédit ou de débit**
- Protection contre les surtensions des serveurs et composants clés de l'infrastructure**

Parlez-en à votre responsable (sécurité) informatique interne ou externe.

Si vous avez besoin d'aide, consultez-nous. Grâce à nos partenariats, nous sommes en mesure de vous indiquer des entreprises spécialisées et expérimentées dans la protection contre les cyber-risques.

# Les prestations d'Helvetia en bref.

## Aperçu des prestations incluses dans les différentes solutions

Propres dommages	Light	Standard	Premium
Restauration du système	✓	✓	✓
Reconstruction des données	✓	✓	✓
Frais supplémentaires pour la poursuite du traitement des données	✓	✓	✓
Perte de gain liée à l'interruption d'exploitation		✓	✓
Analyse du sinistre/analyse forensique		✓	✓
Gestion des notifications			✓
Gestion de la réputation			✓
Paiement de rançon et défense contre le chantage			✓
Compensation de patrimoine en raison d'une cyberfraude ou manipulation			✓
Production de mauvaise qualité		(✓)	(✓)

Sinistres en responsabilité civile	Light	Standard	Premium
Dommages purement économiques et dommages immatériels		✓	✓

Protection juridique	Light	Standard	Premium
Conseil juridique et première intervention		✓	✓

### Combinaison entre propres dommages, sinistres en responsabilité civile et protection juridique

La cyber-assurance Helvetia couvre à la fois les propres dommages, les sinistres en responsabilité civile et les coûts liés à la protection juridique.

En raison de la complexité et de la diversité des sinistres potentiels, Helvetia a défini trois solutions de prestations (Light, Standard et Premium) qui répondent aux différents besoins des entreprises. Chacune de ces solutions combine plusieurs prestations dans les domaines «Propres dommages», «Sinistres en responsabilité civile» et «Protection juridique».

Les entreprises sont ainsi libres de choisir la couverture d'assurance qui correspond le mieux à leur situation en matière de risques et qui leur procure une protection optimale.

### En cas de sinistre, mais aussi en matière de conseil, vous pouvez compter sur notre aide et sur la compétence de notre réseau d'experts

- Conseil en gestion de crise et de communication
- IT-/OT-Security
- Conseil en protection des données/conseil juridique

[www.helvetia.ch/cyber-assurance](http://www.helvetia.ch/cyber-assurance)



### Bon à savoir

En se rendant sur le site Internet d'Helvetia, les PME peuvent évaluer leurs risques en effectuant un test de cybersécurité. Elles trouveront aussi des conseils et recommandations pour améliorer leur protection contre les cyberattaques.

Une formation gratuite sur la sécurité est également disponible en ligne. Les collaborateurs peuvent apprendre comment traiter correctement les données confidentielles, reconnaître les courriers frauduleux et les réflexes à adopter lorsqu'on travaille dans un espace public.

Et en cas de sinistre, notre service des sinistres gratuit vous aidera 24 heures sur 24, 7 jours sur 7.



## Exemples de sinistres.



### Cryptage de données sur un cloud

Une entreprise sauvegarde toutes ses données sur un cloud externe. Un hacker parvient à le pirater et crypte l'ensemble des données stockées à l'aide d'un **rançongiciel**. L'entreprise se trouve dans l'impossibilité d'accéder à ses données et subit de ce fait une interruption de production.

### Dans la mesure où tout cloud externe fait partie du système informatique des entreprises, Helvetia prend en charge les frais suivants

- Restauration des données à partir de la sauvegarde
- Reconstruction manuelle des données qui, techniquement, ne peuvent plus être restaurées à partir de la sauvegarde
- Frais supplémentaires pour le maintien de l'exploitation
- Perte de gain due à l'interruption d'exploitation
- Analyse du sinistre, y compris analyse forensique



### Manipulation de la centrale téléphonique

Un hacker pirate le système de télécommunication d'une entreprise (**phreaking**) et le manipule de telle sorte que des appels téléphoniques très onéreux sont régulièrement passés à l'étranger par des tiers aux frais de cette entreprise. A la fin du mois, celle-ci tombe des nues en recevant une facture téléphonique de plusieurs dizaines de milliers de francs.

### Helvetia rembourse le dommage pécuniaire causé par la manipulation de la centrale téléphonique.



### Piratage des commandes OT

A l'aide d'un courriel frauduleux (social engineering), un hacker pirate les données utilisateur du personnel (**phishing**) dans une entreprise de production ultra-informatisée. Il parvient à pénétrer dans le réseau machines de l'entreprise et à modifier certains paramètres. La manipulation passe d'abord inaperçue, une machine dysfonctionne, d'où une série de produits de mauvaise qualité.

### Helvetia couvre

- les frais d'analyse du sinistre et de restauration des paramètres corrects
- les frais supplémentaires pour le maintien de l'exploitation
- les dommages pécuniaires consécutifs à la série de produits de mauvaise qualité



### Que sont les systèmes OT?

Les systèmes OT (Operational Technology) désignent une grande variété de systèmes de commande (tels que ceux pour la technologie médicale, les techniques de chauffage, de refroidissement et de mesure, ou les systèmes de commande pour la production, le déplacement, la manipulation, la transformation des matériaux, etc.) ainsi que les commandes électroniques faisant partie intégrante d'une machine ou d'une installation.

Les prestations indiquées ici à titre d'exemples dépendent de la solution de prestations choisie.



### Vol de données confidentielles de patients

Un médecin a sauvegardé les données de ses patients sur son propre serveur. En dépit d'un dispositif de sécurité sophistiqué, un hacker parvient à installer un **cheval de Troie** dans le système à l'aide d'un courriel frauduleux. Le médecin met plusieurs semaines à s'en rendre compte, de sorte que le hacker a tout le temps de copier la totalité des données des patients.

#### Helvetia prend en charge les frais suivants

- Analyse du dommage et suppression du logiciel malveillant
- Mesures d'urgence en cas de chantage
- Notification officielle aux personnes concernées qu'il y a potentiellement eu violation de la protection des données
- Gestion de la réputation visant à restaurer la confiance
- Eventuelles demandes en réparation des patients
- Procédure officielle de protection des données

#### Paralysie de la boutique en ligne



A la suite d'une **attaque DoS**, la boutique en ligne de vente de chaussures est paralysée et les clients n'ont plus accès au site Internet. Après quelques jours, l'attaque peut être repoussée avec l'aide d'un spécialiste en informatique. Toutefois, tant que les mesures défensives ne sont pas en place, le magasin de chaussures subira une perte de bénéfices pendant la période de Noël, pic d'activité commerciale.

#### Helvetia prend en charge les frais suivants

- Frais supplémentaires pour le maintien de l'exploitation (p. ex. blackholing, installation d'un géofiltre ou activation d'un disaster recovery site)
- Perte de gain résultant du blocage de la boutique en ligne et de l'interruption des ventes
- Analyse du sinistre, y compris analyse forensique
- Frais engagés pour la gestion de la réputation en vue de restaurer la confiance des clients



### Prétentions en responsabilité civile pour retards de livraison

Un **logiciel malveillant** est installé sur le système informatique de l'entreprise via une clé USB privée d'un collaborateur d'un cabinet d'architecture et crypte toutes les données du serveur. Conséquence: le cabinet n'est plus en mesure de fournir les derniers plans en urgence à la direction du chantier, la construction prend du retard. Plusieurs parties impliquées dans le projet font valoir des prétentions au cabinet d'architecture (machines de construction à l'arrêt, perte de loyer, etc.).

#### Helvetia indemnise

- les prétentions justifiées et défend les prétentions injustifiées des partenaires contractuels de l'architecte
- les frais en lien avec la restauration du système (y c. suppression du maliciel)
- les dépenses de reconstruction manuelle des données qui ne peuvent plus être restaurées à partir de la sauvegarde



#### Découvrir les cyber-risques en version numérique

Scanner le code QR et démarrer.

Helvetia, assureur suisse leader, propose depuis 1858 des solutions d'assurance et de prévoyance sur mesure aux entreprises et clients privés. Helvetia soutient des engagements sociétaux.



Partenaire officiel de Swiss-Ski depuis 2005.



En faveur de la forêt protectrice depuis 2011.

**Helvetia Assurances**

T +41 58 280 10 00 (24h), [www.helvetia.com](http://www.helvetia.com)



**simple. clair. helvetia**   
Votre assureur suisse