HISCOX
Expertise garantie

Cyberassurances d'Hiscox

Votre activité continue, avec une prévention forte et une souscription simplifiée.

www.hiscox.be

Protéger les entreprises de la cyber-menace : un enjeu crucial pour vos clients !

Dans un monde de plus en plus digitalisé, les risques de cyberattaques pesant sur les entreprises augmentent… et, avec eux, les besoins de vos clients de s'en protéger !

Avec les assurances CyberClear d'Hiscox, vous leur offrez cette protection, afin qu'ils ne soient pas seuls face aux cyber-risques.

La cyber-menace, qu'est-ce que c'est ?

- Un salarié d'une entreprise effectue un virement bancaire de 25 000 € à des pirates après s'être fait piéger par un e-mail de phishing prétendument envoyé par un haut dirigeant.
- Les fichiers d'une petite entreprise sont soudainement chiffrés, et elle reçoit une demande de rançon d'un pirate informatique.
- Un salarié oublie dans un train son ordinateur portable qui contient des données à caractère personnel, entraînant une obligation de notification en application du RGPD.
- Un salarié configure mal une mise à jour logicielle pendant un week-end, entraînant une panne des systèmes et une interruption des activités.

Une menace de plus en plus proche et toujours plus onéreuse

- En 2020, près d'une entreprise sur deux a subi une cyber-attaque.*
- Les dommages subis dépassent facilement 10 000 € et s'élèvent même parfois à plusieurs millions d'euros.*
- Dans plus de 15 % des cas, l'attaque a mis en danger la survie de l'entreprise.*

* Chiffres du rapport Hiscox 2021 sur la gestion des cyber-risques.

Ouvrir un mail, c'est un geste quotidien et totalement banal… mais plus aujourd'hui !

Avec un simple email piégé, votre client peut devenir la victime d'un hacker opportuniste ou qui s'intéresse à ses clients. Les conséquences sont multiples :

Conséquences opérationnelles :
temps perdu à résoudre l'incident, chômage technique, etc.

Conséquences réputationnelles :
perte de crédibilité vis-à-vis des clients, etc.

Conséquences financières :
perte de revenus, difficultés de trésorerie, etc.

Ne prenez pas le risque de laisser votre client seul face à un cyber-incident.

Assurance contre la cyber-menace : est-ce vraiment indispensable ?

Oui, parce que dans un monde qui change de plus en plus vite, les risques évoluent aussi… Il est donc essentiel que les couvertures et assurances professionnelles s'adaptent également pour réellement protéger vos clients.

- Parce que les protections techniques sont insuffisantes.
- Parce que les autres assurances professionnelles ne couvrent pas ce risque.

L’assurance cyber et les protections techniques sont complémentaires :

Protections techniques

- Le premier rempart face à un cyber-incident
- Indispensables mais pas infaillibles
- N’empêchent pas une erreur humain

Assurance cyber dédiée

Pour gérer la crise :

- ✓ Sélectionne les meilleurs experts
- ✓ Les mobilise rapidement
- ✓ Paye leurs prestations

Pourquoi les autres assurances ne couvrent-elles pas votre client ?

Seule une assurance cyber assiste votre client en cas de crise, et aide à minimiser les conséquences sur son activité. Couvre uniquement les dommages

L’assurance RC pro ?

Couvre uniquement les dommages subis par un client/tiers qui met en cause la qualité des prestations, mais ne couvre pas les dommages liés à une cyber-attaque subie par une entreprise.

L’assurance tous risques informatiques ?

Couvre uniquement les dommages matériels et leurs conséquences subis par les équipements informatiques, mais ne couvre pas la perte des données, la divulgation d’informations sensibles, etc.

L’assurance fraude ?

Couvre uniquement les conséquences d’actes illicites à l’encontre du client (tels que l’abus de confiance, le faux et usage de faux, l’escroquerie) visant à se faire remettre indument des valeurs ou des biens, mais ne couvre pas notamment la cyber-extorsion ainsi que les atteintes à l’intégrité du système d’information et/ou à celle des données détenues par une entreprise.

Un accompagnement complet face aux cybermenaces. Avant, pendant et après !

Notre assurances CyberClear protègent vos clients à 100 %. Dans tous les domaines et à tout moment... y compris de manière préventive, grâce à de nombreux services et formations, de quoi leur permettre d'être plus forts face aux cybermenaces !

Qu'est-ce qui différencie les assurances CyberClear d'Hiscox des autres produits cyber du marché ?

CyberClear et CyberClear Premium sont des solutions complètes de cyberprotection qui accompagnent vos clients sur les plans technique, juridique, humain, financier… avant, pendant et après une crise !
Avant une crise ? Absolument : Hiscox accompagne déjà vos clients en amont, notamment en formant leurs collaborateurs à tous les aspects de la cybersécurité. Et la police offre à vos clients, pendant et après une crise, des garanties étendues contre les cyber-risques, leur permettant de bénéficier de tout le savoir-faire d'un réseau d'experts.

Quelles couvertures offre une assurance CyberClear ?

La prévention

Nous proposons à vos clients de nombreux services préventifs et des formations, adaptés à la taille de leur entreprise :

- Accès illimité au scan et rapport Hiscox Cyber insight : detection des vulnérabilités et synthèse des recommandations.
- Formations CybSafe pour renforcer la résilience, et tests de phishing pour les collaborateurs.
- Solution Norton Small Business jusqu'à 20 appareils.

L'assistance

- En cas d'incident et sur un simple appel, nous mobilisons immédiatement les spécialistes indispensables pour gérer la globalité de la crise : experts informatiques + avocats spécialistes + spécialistes de la communication de crise
- Sans franchise

Les coûts opérationnels

Nous couvrons les différents frais, coûts et pertes d'exploitation dus à un cyber incident :

- perte de revenus consécutive et coût des mesures correctives mises en place ;
- frais de notification de la violation de données aux régulateurs et aux personnes physiques ;
- frais de récupération des données perdues, volées ou endommagées ;
- credit monitoring ;
- frais d'amélioration ;
- cybervol ;
- cyber-rançon ;
- frais d'avocats et d'enquête face aux régulateurs.

La responsabilité

Nous gérons les réclamations ou sanctions pour préserver votre intérêt commercial :

- dommages causés aux tiers (clients, prospects, fournisseurs, etc.), et notamment les dommages et intérêts suite à une atteinte aux données personnelles et professionnelles, à une transmission de virus…

Les assurances en un coup d'œil

CyberClear

- Seulement deux questions techniques lors de la souscription pour les entreprises dont le chiffre d'affaires peut atteindre 25 millions d'euros: utilisez-vous l'authentification multifacteur (MFA) ou le single sign-on ? Disposezvous d'une sauvegarde, déconnectée ou dans le cloud ?
- CybSafe. Via cette plateforme, les collaborateurs peuvent suivre des formations portant notamment sur le phishing, l'utilisation sécurisée des e-mails, la gestion d'un incident cyber, ainsi que participer à des simulations d'attaques de phishing.
- Accès illimité au scan et rapport Hiscox Cyber insight : detection des vulnérabilités et synthèse des recommandations.
- Un portail self-service pour tout gérer vous-même. Des formations CybSafe aux scans de risques Hiscox Cyber insight, tout est regroupé clairement en un seul endroit.

CyberClear Premium

Identique dans son essence à la CyberClear, mais avec ces suppléments :

✓ logiciel Norton Small Business pour la cybersécurité, adapté jusqu'à 20 appareils ;

✓ sans franchise.

HISCOX CYBER HOTLINE

Numéro de réponse aux incidents 24h/24 :

0800 90255 numéro gratuit, uniquement en Belgique

078 059001 tarif national, joignable en Belgique et à l'étranger avec l'indicatif +32

Des outils pour agir avant une cyber-attaque

Formations préventives, contrôles, scans et logiciel Norton Small Business. Vos clients disposent des meilleurs outils pour se préparer et se protéger contre les cybercriminels !

CybSafe

CybSafe renforce la conscience numérique des collaborateurs via des leçons de sécurité courtes, compréhensibles et directement applicables. Il aide les entreprises à réduire les risques en orientant les comportements, au lieu de se fier uniquement à la technologie.

Ce que les clients y gagnent :

- micro-formations pratiques adaptées aux menaces actuelles, telles que des simulations d'attaques de phishing ;
- une visibilité sur les comportements à risque au sein de l'entreprise, avec un reporting clair ;
- une protection renforcée contre le phishing, les mots de passe faibles et les fuites de données ;
- moins d'incidents et moins d'interruptions dans le fonctionnement quotidien ;
- des mises à jour continues sans complexité technique pour l'utilisateur.

Hiscox Cyber Insight – Scan des vulnérabilités

Scan gratuit des vulnérabilités du site web et de l'informatique visible de l'extérieur. Hiscox Cyber Insight analyse la surface externe de l'environnement IT et cartographie clairement les vulnérabilités. Le client reçoit un rapport concis avec des recommandations concrètes.

Hiscox Cyber Maturity Model

Ce test complet d'évaluation en ligne permet aux entreprises de mesurer facilement leurs capacités de gestion des cyber-risques, et donc de mieux comprendre les forces et faiblesses de leur cybersécurité. Six domaines clés de la cybersécurité sont évalués, à travers les personnes, les processus et la technologie, pour une approche multidimensionnelle. Le modèle interactif de l'outil permet aux entreprises de comparer leurs performances avec celles d'autres acteurs. Outre une notation octroyée à l'entreprise, l'outil explique aux entreprises quelles mesures peuvent prendre les cyber-experts pour améliorer leur cyber-résilience.

Hiscox Cyber Health Check

Notre outil rapide où vous répondez à seulement 7 questions relatives à la cybersécurité pour découvrir quel est le niveau de risque de votre client : faible, moyen ou élevé. Utilisez-le pour lancer avec lui un premier échange sur l'importance des bonnes pratiques de cybersécurité.

Norton Small Business
avec CyberClear Premium

Solution de cybersécurité spécialement conçue pour les petites entreprises, qui aide à mieux sécuriser les appareils et les données face à des menaces telles que les virus, les malwares et le phishing. Avec comme fonctions principales :

- ✓ device security : antivirus et firewall ;
- ✓ cloud backup gratuit : récupération en cas de rançongiciel ou perte de données ;
- ✓ VPN gratuit : connexions sécurisées, même sur les réseaux publics ;
- ✓ software updater : signale les logiciels obsolètes et les mises à jour ;
- ✓ password manager : gestion sécurisée des mots de passe ;
- ✓ business customer support : assistance en français pour les questions sur le logiciel de sécurité ;
- ✓ business tech support : aide pour les problèmes informatiques généraux ;
- ✓ monitoring des comptes financiers et médias sociaux.

Par client, jusqu'à 20 appareils peuvent être protégés.

Garantie supplémentaire :
avance forfaitaire journalière

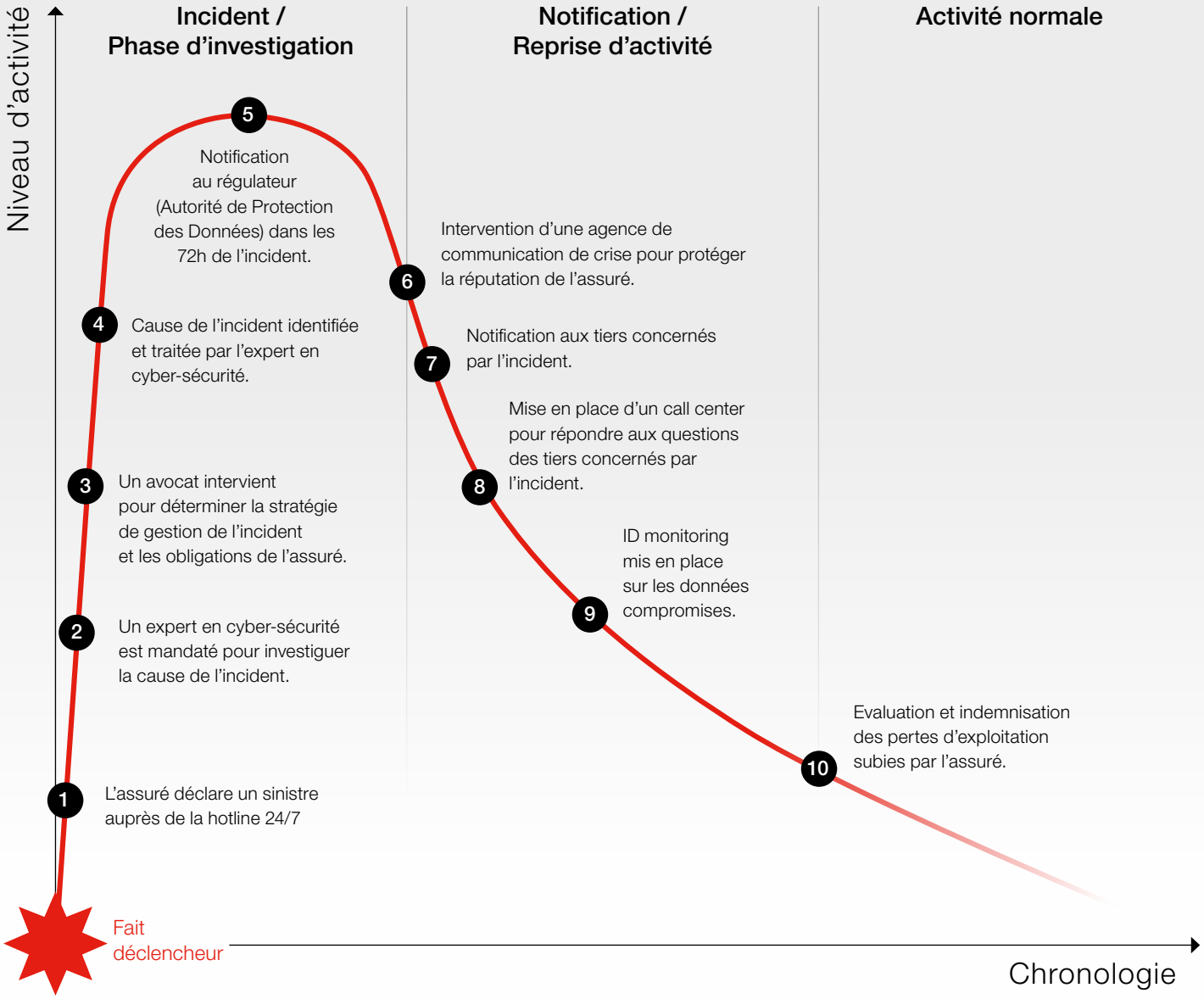
Les PME réalisant un chiffre d'affaires jusqu'à 2,5 millions d'euros bénéficient d'une avance forfaitaire quotidienne pendant maximum 30 jours, versée sans attendre l'évaluation des pertes réelles. Ce soutien financier immédiat vous permet de faire face rapidement aux dépenses urgentes et de maintenir votre activité.

Par la suite, les pertes réelles sont réévaluées et ce sans surprime. Vous êtes alors indemnisé à hauteur du montant exact de vos pertes, sans toutefois pouvoir dépasser le plafond de garantie. Ainsi, vous avez la certitude d'être accompagné de façon juste et conforme à vos besoins réels.

Ce que nous faisons pour vos clients en cas de crise

Dès qu'une crise survient, nous prenons les choses en main pour vos clients. Et pour un maximum d'efficacité, notre intervention est minutieusement préparée pour leur offrir une protection allant dans les moindres détails.

Hiscox s'occupe de tout :
nos experts escortent vos clients depuis la déclaration du cyber-incident jusqu'à sa résolution



7 bonnes raisons de proposer une assurance CyberClear d'Hiscox à vos clients

1 Hotline 24h/24 et 7j/7 : nous offrons à nos assurés une assistance SANS FRANCHISE pour les aider au mieux pendant un cyberincident, via hiscox.claims@hiscox.be et au 0800 90255 (numéro gratuit, uniquement en Belgique) ou 078 059001 (tarif national, accessible en Belgique et internationalement avec l'indicatif +32)

2 Simplicité : Une assurance CyberClear d'Hiscox est tout simplement… clair. Vous savez ce contre quoi votre client est couvert.

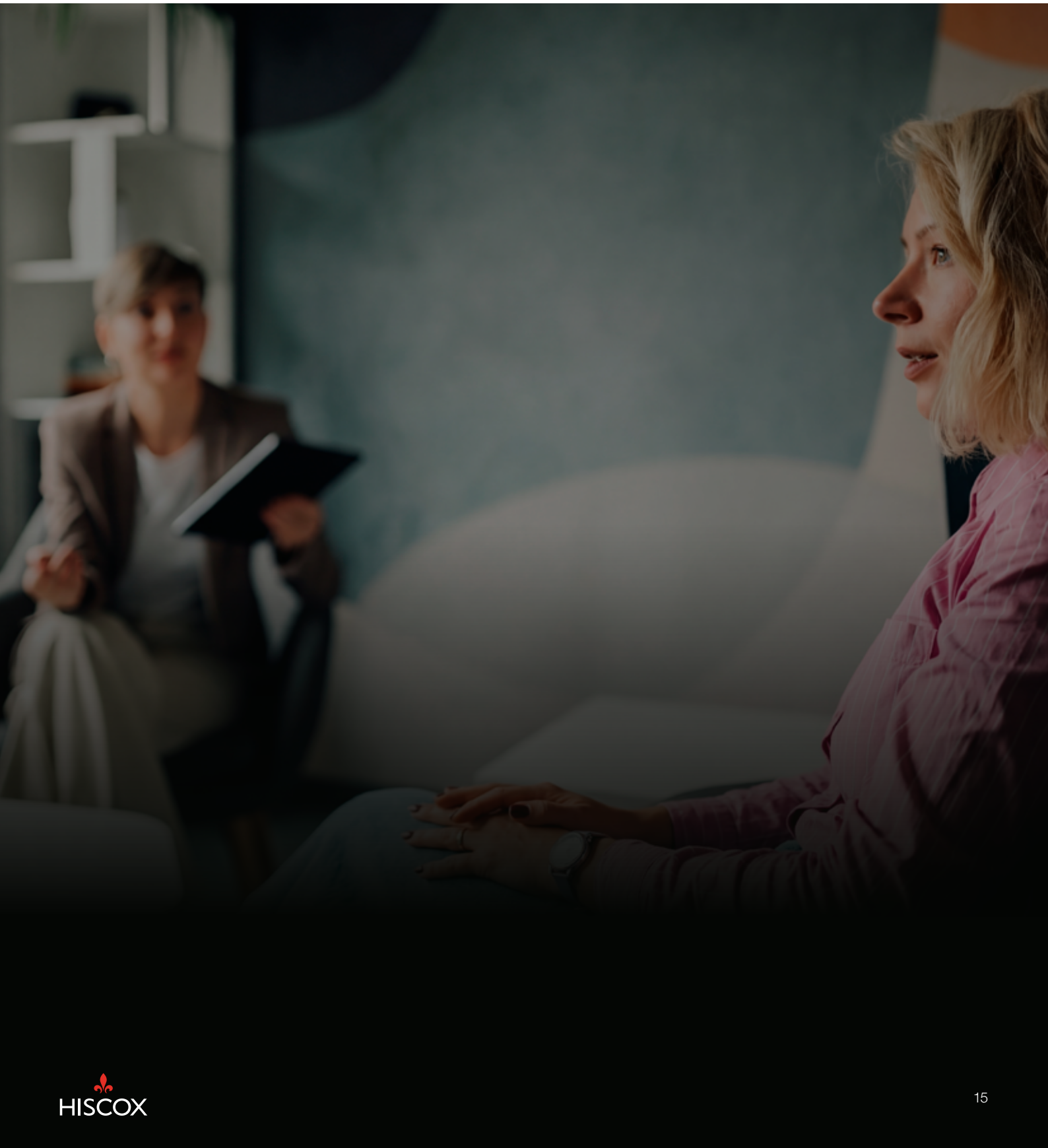
3 Accès aux meilleurs experts du secteur : experts de la sécurité informatique, avocats spécialisés en protection des données et experts en gestion de crise…

4 10 ans d'expérience en cyber-assurance : nous savons ce que nous faisons !

5 Pérennité : CyberClear by Hiscox ne couvrira pas uniquement les risques que votre client court aujourd'hui. Nos polices sont particulièrement complètes et les protègent des risques, menaces et attaques numériques émergents que les criminels pourraient mettre au point dans les années à venir.

6 Plus de 220 000 clients satisfaits en Europe.

7 Souscription simple et rapide : votre client est assuré en quelques minutes, via une proposition pré-tarifiée (PPP, « pre-priced proposal ») ou directement via notre portail destiné aux courtiers en assurances.



Leur histoire, notre intervention

Découvrez à travers ces 4 exemples comment Hiscox intervient et libère vos clients des pièges cyber.

Un phishing trip qui coûte cher

Secteur Agroalimentaire
Chiffre d'affaires + 40m €
Coût du sinistre 49 000 €

Un salarié d'une société dans le secteur agroalimentaire a été victime d'un phishing, en recevant un faux email d'un haut dirigeant de la société qui lui demandait de transférer 49 000 € sur un compte bancaire désigné. Croyant la demande authentique, le salarié a débloqué les fonds et ni la banque de la société, ni la banque destinataire n'ont réussi à recouvrer les fonds. L'e-mail en question provenait en réalité d'un compte Gmail créé pour imiter la véritable adresse du dirigeant

Prise en charge d'Hiscox

En réalisant ce qui s'était passé, la société nous a appelé et nous avons immédiatement dépêché un expert des failles et une société spécialisée dans la sécurité informatique pour déterminer si les systèmes de l'assuré présentaient une faille ou si des données à caractère personnel avaient été compromises. Nous avons remboursé l'argent perdu dans un délai d'un mois à compter de la déclaration. En l'espèce, aucune faille de données ne s'était produite donc aucune notification n'était nécessaire. En tant que garantie complémentaire, une couverture jusqu'à 50 000 euros peut être offerte pour les pertes en cas de détournement de paiements.

Une société informatique piégée

Secteur Technologie
Chiffre d'affaires + 40m €
Coût du sinistre 70 000 €

Une société de technologie a remarqué qu'un malware avait été installé sur l'un de ses serveurs.

Prise en charge d'Hiscox

Nous avons immédiatement sollicité notre expert en sécurité informatique pour analyser les fonctions du malware et enquêter sur les circonstances de son apparition dans les systèmes de notre client. Le serveur contenait un volume important de données à caractère personnel. C'est pourquoi nous avons cherché à savoir s'il existait une faille plus importante ou un risque que ces données aient été compromises. Compte tenu de la gravité potentielle de la faille, nous avons dépêché un expert de la protection des données pour superviser l'enquête. L'analyse a confirmé que le malware était un programme de minage, heureusement, rien de trop grave : aucune autre fuite de données n'a été détectée.

Une note salée pour le restaurant

Secteur Services de restauration
Chiffre d'affaires 0-10m €
Coût du sinistre 29 000 €

Une attaque par ransomware a chiffré l'intégralité du système informatique d'un restaurant, affectant jusqu'à ses caisses physiques et rendant toute transaction impossible.

Prise en charge d'Hiscox

Ayant épuisé toutes les autres options, il est apparu que le moyen le plus efficace pour rétablir les systèmes de l'établissement était de payer la rançon. Nous avons donc pris en charge le coût de la rançon, ainsi que les coûts informatiques liés à la mise en œuvre du déchiffrement et à la restauration complète des fonctionnalités du système. Nous avons également dépêché notre expert pour détecter d'éventuelles violations de données personnelles. En plus de ces coûts, nous avons compensé la perte d'exploitation subie par le restaurant du fait de son incapacité temporaire à exercer son activité.

Les publicitaires et le Bitcoin

Secteur Marketing
Chiffre d'affaires 0-1m €
Coût du sinistre 44 000 €

Une société de relations publiques a remarqué un problème affectant ses courriers électroniques. Son sous-traitant informatique habituel a enquêté et déterminé que la cause la plus probable était une activité malveillante. L'assuré nous a alors contacté et nous avons dépêché sur site notre expert en sécurité informatique, qui a confirmé que l'assuré était victime d'une attaque. Les systèmes informatiques de la société étaient infectés par un programme de cryptojacking destiné au minage de cryptomonnaie. L'enquête a également pu déterminer que les hackers qui avaient déployé ce malware avaient pénétré les systèmes de l'assuré et potentiellement menacé l'intégrité de données à caractère personnel.

Prise en charge d'Hiscox

Après avoir enquêté pour déterminer la gravité de l'intrusion, notre expert informatique a désinstallé le logiciel malveillant et remédié aux failles de sécurité dans les systèmes. Nous avons mandaté notre cabinet d'avocats experts afin d'accompagner notre client dans ses obligations de notification et avons effectué les notifications aux autorités de régulation et aux personnes concernées.

FAQ

Pourquoi souscrire une police de cyber-assurance ?

Vos clients sont très probablement assurés contre les risques tels que les incendies, inondations et la négligence professionnelle, mais ils ont autant de risque (voire plus) de subir une cyber-attaque. Ces attaques peuvent entraîner une perte d'activités, du chiffre d'affaires et une atteinte à leur réputation, ainsi que des coûts importants pour gérer l'attaque et des sanctions financières.

Les assurances professionnelles ne couvrent-t-elle pas déjà ce risque ?

Non. Les assurances professionnelles standards n'offrent pas une protection complète. C'est pourquoi vos clients ont besoin d'une cyber-assurance.

Votre client ne pense pas être la cible des hackers…

Beaucoup d'activités criminelles en ligne ne visent pas spécifiquement une entreprise particulière. Les responsables des attaques utilisent souvent des outils qui recherchent sur Internet les systèmes vulnérables. Les hackers exploiteront alors cette vulnérabilité, sans se soucier de la victime derrière.

Votre client n'a pas d'activités en ligne. Cette assurance a-t-elle un intérêt pour lui ?

De nombreuses entreprises se considèrent « hors ligne » et pensent donc ne pas avoir besoin d'une cyber-assurance. Néanmoins, selon une enquête, 94 % des entreprises ont aujourd'hui intégré la nécessité d'utiliser un service en ligne : envoi d'e-mail ou recherche en ligne par le personnel, usage de services bancaires ou plateformes d'achat en ligne destinées à leurs clients… De fait, celles-ci sont exposées aux risques cyber.

Votre client ne détient pas de données à caractère personnel. A-t-il tout de même besoin de cette assurance ?

La définition des données à caractère personnel au sens du RGPD est très large. Elle comprend par exemple les adresses e-mail professionnelles. Votre client doit également considérer les informations de ses fournisseurs et celles de ses salariés (passés, présents et personnes adressant une candidature). De plus, la plupart des sinistres que nous traitons n'impliquent pas de violation des données à caractère personnel, mais une perte d'exploitation, une altération des données ou une interruption du système. Autant de situations auxquelles votre client peut être confronté, même s'il ne détient pas beaucoup de données à caractère personnel.

Est-ce que cette assurance protège uniquement contre les attaques informatiques ?

Non. Si la cybercriminalité constitue la principale source de sinistres, les erreurs humaines peuvent également être à l'origine de problèmes. Par exemple : envoi d'un e-mail au mauvais destinataire, oubli d'un attaché-case dans un train ou mauvaise configuration d'un système.

Qu'est-ce qui distingue une assurance CyberClear des autres produits cyber sur le marché ?

Les assurances CyberClear sont des solutions complètes de cyberprotection qui accompagne vos clients sur les plans technique, juridique, humain, financier… pendant et après la crise. Hiscox les accompagne aussi en amont, notamment en formant leurs salariés à la cyber-sécurité. La police leur offre des garanties larges contre les cyber-risques et leur permet de bénéficier de l'expertise d'un réseau d'experts tout au long de la durée de leur contrat.

Encore des questions ?
Nous sommes heureux d'y répondre !

Contactez-nous :
+32 (0)2 788 26 00
hiscox.underwriting@hiscox.be

Ombudsman des Assurances :
Square de Meeûs 35, 1000 Bruxelles Tél. : 00 32 (0) 25 47 58 71
E-mail : info@ombudsman-insurance.be www.ombudsman-insurance.be