Questionnaire sur les risques cyber (étendu)

Introduction

Le **questionnaire standard sur les risques cyber** doit être complété lorsque
- la somme d'assurance souhaitée pour propres dommages/somme d'assurance combinée est supérieure à CHF 500'000; ou
- la somme d'assurance souhaitée pour responsabilité civile est supérieure à CHF 1 Mio.

Si un ou plusieurs des critères suivants est/sont rempli(s), le **questionnaire étendu sur les risques cyber** doit être complété:
- la somme d'assurance souhaitée pour propres dommages/somme d'assurance combinée est supérieure à CHF 1 Mio;
- la somme d'assurance souhaitée pour la responsabilité civile est supérieure à CHF 2 Mio;
- le chiffre d'affaires cumulé de toutes les entreprises coassurées est supérieur à CHF 100 Mio.

Les questions relatives aux risques se rapportent au proposant/à la proposante, y compris à l'ensemble des entreprises coassurées. Veuillez mentionner, si les réponses aux questions ne s'appliquent qu'à une partie du proposant/de la proposante et des entreprises coassurées. En cas de divergences importantes, il est recommandé de remplir un questionnaire par entreprise.

1. Mesures de protection organisationnelles

1.1 Organisation informatique

Avez-vous désigné une personne interne ou externe responsable de l'informatique au sein de votre entreprise? ☐ Oui ☐ Non

Si oui: nom et fonction (pour une personne externe, veuillez préciser le nom de l'entreprise pour laquelle elle travaille)

Avez-vous désigné une personne interne ou externe responsable de la sécurité informatique au sein votre entreprise? ☐ Oui ☐ Non

Si oui: nom et fonction (pour une personne externe, veuillez préciser le nom de l'entreprise pour laquelle elle travaille)

Existe-t-il une répartition claire des tâches entre le ou la responsable de l'informatique et le ou la responsable de la sécurité informatique, ou s'agit-il de la même personne?

☐ Les tâches sont clairement réparties ☐ Il s'agit de la même personne

Combien de temps êtes-vous en mesure de maintenir votre activité en cas de défaillance des systèmes informatiques indispensables au bon fonctionnement de votre entreprise?

☐ Arrêt immédiat

☐ Jusqu'à 12 h ☐ Jusqu'à 24 h

☐ Jusqu'à 36 h ☐ Plus de 36 h

1.2 Gestion des utilisateurs, gestion des autorisations et directives concernant les mots de passe

Chaque utilisateur dispose-t-il de son propre compte? ☐ Oui ☐ Non

Les utilisateurs ont-ils des niveaux d'autorisation/droits d'accès différents dans les systèmes informatiques selon leur fonction et les tâches qui leur sont assignées (y compris droits d'administrateur [accès lié à la fonction à des données financières, personnelles ou de clients, p. ex.])? ☐ Oui ☐ Non

Mettez-vous en place des droits d'administration gradués afin d'empêcher/rendre plus difficile les attaques de déplacement latéral? ☐ Oui ☐ Non

Avez-vous défini et implémenté une politique de mots de passe permettant de garantir des mots de passe solides? ☐ Oui ☐ Non

Si oui: quelle est la fréquence de renouvellement des mots de passe?

☐ Tous les 3 mois ☐ Tous les 6 mois

☐ Tous les 12 mois ☐ Tous:

Les demandes d'accès sont-elles bloquées sur l'ensemble des systèmes après un certain nombre d'échecs de connexion défini en interne et les administrateurs en sont-ils informés? ☐ Oui ☐ Non

Si oui: après combien tentatives?

Existe-t-il un dispositif empêchant systématiquement les utilisateurs d'installer des programmes sur les terminaux? ☐ Oui ☐ Non

1.3 Sensibilisation

L'ensemble des utilisateurs informatiques de l'entreprise assurée suivent-ils des formations/séminaires sur le thème de la sensibilisation aux cyber-risques?

☐ Oui, une fois (p. ex. au moment de l'entrée dans l'entreprise)

☐ Oui, les formations/séminaires ont lieu de manière irrégulière (moins d'une fois par an)

☐ Oui, les formations/séminaires ont lieu régulièrement (au moins une fois par an)

☐ Non

Des simulations d'hameçonnage (phishing) sont-elles utilisées pour sensibiliser? ☐ Oui ☐ Non

1.4 Analyse des risques et des vulnérabilités/certifications

Avez-vous au cours des 3 dernières années effectué/fait effectuer une analyse des risques et des vulnérabilités de votre sécurité informatique (tests d'intrusion/détection de vulnérabilités ou audits de sécurité, p. ex.)?

☐ Oui, ce qui a permis d'identifier et de traiter des failles critiques

☐ Oui, ce qui a permis d'identifier des failles critiques qui n'ont pas encore été traitées ou corrigées

☐ Oui, mais aucune faille critique n'a été identifiée

☐ Non

Dans le cas où des failles critiques n'ont pas encore été traitées ou corrigées: dans quels délais est-il prévu d'y remédier?

☐ Dans les 6 mois à venir

☐ Dans plus de 6 mois, veuillez en indiquer la raison:

Des analyses des risques et des vulnérabilités sont-elles régulièrement effectuées? ☐ Oui ☐ Non

Si oui: quelles analyses/tests?

À quelle fréquence?

Existe-t-il un processus d'amélioration continue dans le domaine de la gestion des risques informatiques? ☐ Oui ☐ Non

L'entreprise dispose-t-elle d'une certification/d'un label pour ce qui relève de la sécurité informatique? ☐ Oui ☐ Non

Si oui: lesquels? (Plusieurs réponses possibles)

☐ ISO / IEC 27001 ☐ ISO 22301

☐ PCI DSS ☐ Cyber-Safe.ch

☐ ISIS12 ☐ SOC II

☐ Autres:

1.5 Vérification des transactions financières et des commandes de produits

Dans le cas de transactions financières d'envergure (factures ou ordres de paiement > CHF 30'000), vérifiez-vous l'authenticité de l'ordre de transaction lorsque les destinataires des virements et/ou les coordonnées bancaires ou de paiement sont nouvelles ou modifiées? ☐ Oui ☐ Non

Si oui: comment vérifiez-vous l'authenticité?

Dans le cas de grosses commandes de produits (> CHF 30'000), en vérifiez-vous l'authenticité? ☐ Oui ☐ Non

Si oui: comment vérifiez-vous l'authenticité?

2. Mesures de protection techniques

2.1 Sauvegarde des données et des systèmes (back-up)

Au sein de votre entreprise, procédez-vous à une sauvegarde quotidienne de vos données? ☐ Oui ☐ Non

Si non: à quelle fréquence et pourquoi pas quotidiennement?

Êtes-vous informé·e de la réussite ou de l'échec de vos sauvegardes (monitoring)? ☐ Oui ☐ Non

Procédez-vous de temps à autre à des simulations de restauration des données issues de vos sauvegardes (Disaster Recovery)? ☐ Oui ☐ Non

Si oui: à quelle fréquence?

Vérifiez-vous la qualité des sauvegardes au minimum tous les 6 mois (volumétrie comparative ou échantillonnage des données aux fins de vérification de la fonctionnalité, p. ex.)? ☐ Oui ☐ Non

Si non: à quelle fréquence et pourquoi pas tous les 6 mois?

Conservez-vous la sauvegarde en lieu sûr, afin qu'elle ne puisse pas être manipulée, endommagée, détruite ou volée en même temps que les originaux (sauvegardes off site et offline, p. ex., ou autres copies de sécurité inaltérables)? ☐ Oui ☐ Non

Les sauvegardes externalisées sont-elles conservées sous forme cryptée? ☐ Oui ☐ Non

Est-il garanti que les fichiers de logs des systèmes critiques (logiciel de comptabilité, contrôleur de domaine, pare-feu, serveur de messagerie, p. ex.) sont conservés et sauvegardés de manière centralisée pendant au moins 6 mois? ☐ Oui ☐ Non

2.2 Logiciels antimaliciels et protection d'accès

2.2.1 Pare-feu, antivirus et antivirus de nouvelle génération (NGAV)

Vos réseaux sont-ils protégés par un pare-feu mis à jour régulièrement? ☐ Oui ☐ Non

Votre réseau informatique est-il segmenté en différents sous-domaines (le département Finance est-il, p. ex., isolé du Développement produits) et les passerelles entre eux sont-elles protégées par un pare-feu? ☐ Oui ☐ Non

Avez-vous installé (dans la mesure du possible) sur l'ensemble des terminaux et des serveurs une solution antivirus mise à jour régulièrement?

☐ Oui ☐ Non

☐ En partie, les terminaux restants disposent d'une protection équivalente (isolement, p. ex.)

Si oui: la solution antivirus est-elle gérée de manière centralisée? ☐ Oui ☐ Non

Avez-vous un antivirus de nouvelle génération (NGAV) ou une solution endpoint detection and response (EDR) en place (Sentinel One, Symantec EDR, p. ex.)?

☐ Oui, pour les terminaux

☐ Oui, pour le·s serveur·s

☐ Non

2.2.2 Accès à distance au réseau de l'entreprise

Est-il possible d'accéder à distance au réseau de l'entreprise? ☐ Oui ☐ Non

Si oui: comment ces accès sont-ils protégés? Il existe un accès à distance:

☐ sans protection d'accès

☐ protégé par un nom d'utilisateur et un mot de passe

☐ protégé par une authentification multifactorielle

Si oui: les tiers qui ont accès au réseau de l'entreprise s'engagent-ils par contrat à assurer un certain niveau de protection de base de votre propre informatique? ☐ Oui ☐ Non

2.2.3 Services en nuage

Utilisez-vous des services en nuage? ☐ Oui ☐ Nein

Si oui: un ou plusieurs de ces services en nuage ont-ils une importance critique* pour votre entreprise? ☐ Oui ☐ Nein

*Sont considérés comme services en nuage critiques pour l'entreprise, les services utilisés pour les processus commerciaux principaux et dont la disponibilité dépend de plus de 30 % du chiffre d'affaires annuel.

Si oui: lesquelles?

Comment sont protégés les accès aux services en nuage d'importance critique pour l'entreprise?
Il existe un accès en nuage:

☐ sans protection d'accès

☐ protégé par un nom d'utilisateur et un mot de passe

☐ protégé par une authentification multifactorielle

Le prestataire externe qui vous propose les services en nuage d'importance critique pour votre entreprise dispose-t-il d'un plan d'urgence et d'un plan de continuité d'activité (BCA, [Business Continuity Plan]) permettant une reprise rapide de vos activités en cas de cyber-incident affectant le prestataire externe?

☐ Oui ☐ Non

☐ Non connu

2.2.4 Autres services disponibles via Internet

Utilisez-vous d'autres services disponibles via Internet: banque en ligne, portail de messagerie, systèmes de billetterie, p. ex.? ☐ Oui ☐ Non

Si l'authentification multifactorielle est disponible pour ces services, est-elle utilisée?

☐ Oui ☐ Non

☐ En partie

2.2.5 Contrôle réseau/inventaire

Seuls les appareils autorisés et enregistrés peuvent-ils se connecter au réseau interne (Network access control, NAC)? ☐ Oui ☐ Non

2.2.6 Operation technology (OT)

Utilisez-vous operation technology* pour vos activités? ☐ Oui ☐ Non

*Operation technology [OT] = contrôles de machines, installations et appareils, comme des installations industrielles reliées au réseau de l'entreprise pour la production ou la fabrication, un entrepôt grande hauteur ou des appareils médicaux, p. ex.

Si oui: les deux réseaux (IT et OT) sont-ils clairement séparés (segmentation des réseaux) et les passerelles entre les réseaux (interfaces logiques ou physiques) sont-elles protégées par des dispositifs (pare-feu, p. ex.) à la pointe de la technologie? ☐ Oui ☐ Non

Est-ce que l'OT dispose d'un accès à distance pour les fabricants ou les employés? ☐ Oui ☐ Non

Si oui: comment les accès sont-ils protégés? Il existe un accès à distance:

☐ sans protection d'accès

☐ protégé par un nom d'utilisateur et un mot de passe

☐ protégé par une authentification multifactorielle

2.3 Gestion des correctifs

Existe-t-il une gestion des correctifs et des mises à jour garantissant que les derniers correctifs/dernières mises à jour de sécurité sont installés rapidement (c.-à-d. dans les 30 jours au plus tard, sauf si le processus de vérification de la compatibilité des correctifs nécessite davantage de temps)? ☐ Oui ☐ Non

Si oui: à l'exception des installations et des appareils qui sont «out of support»: ces installations et appareils (IT et/ou OT) qui ne bénéficient plus de correctifs/mises à jour de sécurité sont-ils rattachés à des réseaux isolés en conséquence et sans connexion avec les systèmes d'importance critique pour l'entreprise? ☐ Oui ☐ Non

Existe-t-il des processus permettant l'installation rapide des mises à jour d'urgence, qui doivent être installées de manière urgente et immédiate selon le fabricant (emergency patch)?

☐ Oui, en l'espace de 12 heures ☐ Oui, en l'espace de 24 heures

☐ Oui, en l'espace de 48 heures ☐ Non

2.4 Administration système

Utilisez-vous un système pour la mise à disposition centralisée de systèmes d'exploitation et la distribution centralisée d'applications? ☐ Oui ☐ Non

2.5 Détection d'intrusion et monitoring

Les évènements réseau, les défaillances système et les incidents de sécurité sont-ils surveillés au moyen d'un système de monitoring? ☐ Oui ☐ Non

Si oui:

☐ par le service informatique interne: aux heures de bureau

☐ par le service informatique interne: 24h/24 et 7j/7 avec service de piquet

☐ par un partenaire externe dédié pour les services de monitoring et de sécurité opérationnelle (Security Operations Center – SOC): aux heures de bureau

☐ par un partenaire externe dédié pour les services de monitoring et de sécurité opérationnelle (Security Operations Center – SOC): 24h/24 et 7j/7 avec service de piquet

Utilisez-vous un système centralisé de collecte des informations de sécurité (SIEM)? ☐ Oui ☐ Non

2.6 E-commerce, boutique et commerce en ligne

Pour le cas où des activités sont réalisées par le biais d'e-commerce/d'une boutique ou d'un commerce en ligne:

Comment protégez-vous votre boutique/commerce en ligne contre les attaques et les interruptions?

☐ Web Application Firewall (WAF) ☐ Distributed Denial of Service (DDoS)

☐ Vulnerability Scans ☐ Possibilité de migrer sur une autre plateforme

☐ Autres:

Votre boutique/commerce en ligne est-il régulièrement soumis à un test de pénétration pour détecter les vulnérabilités actuelles (au moins une fois par an)? ☐ Oui ☐ Non

Qui est responsable pour le traitement des transactions financières dans votre boutique/commerce en ligne?

☐ Un prestataire de services de paiement ☐ Nous-mêmes

Existe-t-il un lien direct entre votre boutique/commerce en ligne et le système informatique (ERP, système de gestion des marchandises, p. ex.)? ☐ Oui ☐ Non

Si oui: cette connexion est-elle sécurisée? ☐ Oui ☐ Non

2.7 Protection contre les surtensions

Les serveurs et autres composants d'infrastructure centraux importants (tels que les routeurs ou systèmes de sauvegarde) sont-ils protégés contre les dommages dus aux surtensions (notamment à par un filtre de surtension approprié ou un système d'alimentation sans interruption [ASI])? ☐ Oui ☐ Non

3. Protection des données

Votre entreprise a-t-elle un ou une responsable de la protection des données (un ou une préposé·e à la protection des données ou un·e Chief Data Officer [CDO], p. ex.)? ☐ Oui ☐ Non

Combien de données de personnes telles que adresse, nom, adresse courriel ou numéro de téléphone (sans les données des employés) enregistrez ou traitez-vous?

☐ Aucune ☐ < 50 K

☐ < 100 K ☐ < 500 K

☐ < 1 Mio ☐ > 1 Mio

Avez-vous accès à des données sensibles*, en conservez-vous ou en traitez-vous (hors données du personnel)? ☐ Oui ☐ Non

*En vertu des dispositions légales en vigueur sur la protection des données, on entend par données sensibles notamment les informations relatives à l'état de santé, l'appartenance d'une personne à une race, les informations relatives aux opinions ou activités religieuses ou politiques, ou encore celles relevant de la sphère intime.

Permettez-vous à vos clients ou vos partenaires commerciaux de payer par carte de crédit? ☐ Oui ☐ Non

Si oui: respectez-vous les exigences des normes PCI-DSS (Payment Card Industry Security Standard)? ☐ Oui ☐ Non

Si vous permettez les paiements de ce type, externalisez-vous entièrement le traitement des données de cartes de crédit et des paiements à un prestataire de services de paiement, de telle manière que les données de cartes de crédit n'apparaissent jamais en totalité (les 4 derniers chiffres au maximum) dans votre réseau d'entreprise ou vos systèmes informatiques? ☐ Oui ☐ Non

Pouvez-vous avec vos systèmes effectuer des transactions financières à partir de comptes de tiers? ☐ Oui ☐ Non

Cryptez-vous les données sur les supports de données de vos appareils? (Plusieurs réponses possibles)

☐ Oui, pour les terminaux

☐ Oui, pour le·s serveur·s

☐ Non

Les données sensibles sont-elles cryptées lors de l'envoi (p. ex. en utilisant un VPN ou le protocole HTTPS, sous forme de courriel crypté, ou en utilisant des supports de données cryptés)? ☐ Oui ☐ Non

Remplissez-vous déjà les obligations suivantes en relation avec la Loi sur la Protection des Données (PD) révisée?
(Veuillez cocher ce qui convient)

☐ Un inventaire du traitement des données est disponible et vérifié chaque année

☐ Un processus écrit de notification des fuites de données est disponible

☐ Une analyse d'impact relative à la protection des données est disponible

☐ Une déclaration de confidentialité figure sur votre site Internet si des données personnelles y sont traitées (cookies, p. ex.)

☐ Les exigences légales en matière de protection des données (anonymisation des adresses IP, p. ex.) lors de l'utilisation d'outils analytiques (Google Analytics, p. ex.) sont connues et appliquées

Des mesures de protection adéquates sont-elles prévues dans votre entreprise contre l'accès physique de tiers à votre infrastructure (ordinateurs, serveurs, réseau)? ☐ Oui ☐ Non

4. Comportement en cas de sinistre

4.1 Plan d'urgence

Avez-vous défini un plan d'urgence en cas de cyber-incident (Emergency Response Plan)? ☐ Oui ☐ Non

Si oui: le testez-vous à intervalles réguliers (au minimum une fois par an)? ☐ Oui ☐ Non

A-t-on établi un plan d'alerte pour savoir qui doit être alerté en cas d'incident cybernétique? ☐ Oui ☐ Non

Les instances nécessaires ont-elles été définies pour mettre en œuvre le plan d'urgence? ☐ Oui ☐ Non

L'équipe «emergency réponse» (ERT) dispose-t-elle des pouvoirs et autorisations de signature nécessaires pour pouvoir agir en cas de sinistre? ☐ Oui ☐ Non

Un concept de communication d'urgence a-t-il été mis sur pied et testé? ☐ Oui ☐ Non

En combien de temps êtes-vous en mesure de restaurer vos systèmes sur un système de secours après une défaillance totale?

☐ En l'espace de 24 heures ☐ En l'espace de 48 heures

☐ En l'espace 72 heures ☐ En l'espace de 1 semaine

☐ En l'espace de 2 semaines ☐ Autre:

4.2 Gestion de la continuité des activités

Disposez-vous d'un plan écrit (Business Continuity Management Plan – BCM) pour maintenir l'activité de l'entreprise en cas de défaillance de votre informatique? ☐ Oui ☐ Non

Si oui: le testez-vous à intervalles réguliers (au minimum une fois par an)? ☐ Oui ☐ Non

Existe-t-il des solutions de rechange/des redondances pour les systèmes informatiques d'importance critique? ☐ Oui ☐ Non

4.3 Incident Responder

Collaborez-vous avec un Incident Responder externe en cas d'incident, avec qui vous planifiez la gestion de crise, effectuez à des tests d'urgence et qui vous aide à gérer efficacement une cyberattaque afin de pouvoir reprendre rapidement vos opérations? ☐ Oui ☐ Non

Si oui: avec qui travaillez-vous?

Si non: disposez-vous en interne d'une équipe Incident Responding à même d'assumer les tâches susmentionnées? ☐ Oui ☐ Non

Protection des données

Toutes les données à caractère personnel sont traitées conformément à la législation sur la protection des données en vigueur. Vous trouverez les dernières informations à ce sujet sur notre page Internet «Notice explicative sur la politique en matière de protection des données» disponible à l'adresse www.helvetia.ch/protectiondesdonnees.

Déclaration de consentement

Les réponses aux questions doivent être complètes et conformes à la vérité. Si cela est nécessaire à l'examen de la proposition ou de la prestation en raison de l'étendue du risque, les données sont transmises à des fins de traitement aux tiers participant au contrat en Suisse et à l'étranger, en particulier aux réassureurs ainsi qu'aux sociétés du Groupe Helvetia, dans le respect de la loi sur la protection des données suisse.

Le/la proposant·e autorise Helvetia, en vue d'atteindre les buts mentionnés dans la notice explicative sur la protection des données, à se procurer auprès des autorités, d'autres compagnies d'assurance et de tiers ainsi que de leurs auxiliaires toute information, donnée et copie de document pertinente le/la concernant (y compris des renseignements portant sur son état de santé antérieur) et, dans ce cadre, à transmettre à ces tiers les informations nécessaires. Le/la proposant·e délie par conséquent expressément ces tiers et Helvetia de leur secret de fonction et professionnel et de toute obligation de confidentialité, et il/elle autorise ces derniers à donner à Helvetia les renseignements nécessaires et à lui remettre tous les documents pertinents pour l'examen de la proposition, l'exécution du contrat et le règlement des cas de prestations.

Les données reçues peuvent être utilisées par les sociétés du Groupe Helvetia ainsi que par leurs sociétés partenaires pour soumettre des offres de prestations de service personnalisées.

Cette autorisation est valable indépendamment de la naissance du contrat et sans limitation dans le temps. Elle peut être révoquée à tout moment par une déclaration sous forme de texte (p. ex. par courriel) à l'attention d'Helvetia. Toute révocation s'applique uniquement pour le futur. Pour autant que l'autorisation soit nécessaire à la préparation ou à l'exécution du contrat, sa révocation n'est possible que par le biais du retrait de la proposition ou de la résiliation du contrat conformément aux dispositions applicables. Une révocation ultérieure peut entraîner l'impossibilité de fournir des prestations. Helvetia est autorisée à poursuivre le traitement des données même en cas de révocation dans la mesure où la loi l'y autorise ou en cas d'intérêt prépondérant.

Les obligations énoncées dans les conditions d'assurance s'appliquent indépendamment des réponses fournies par le/la proposant·e dans le présent questionnaire.

Le/la proposant·e

Nom du proposant/de la proposante:

Nom et fonction du signataire:

Lieu, date

Signature