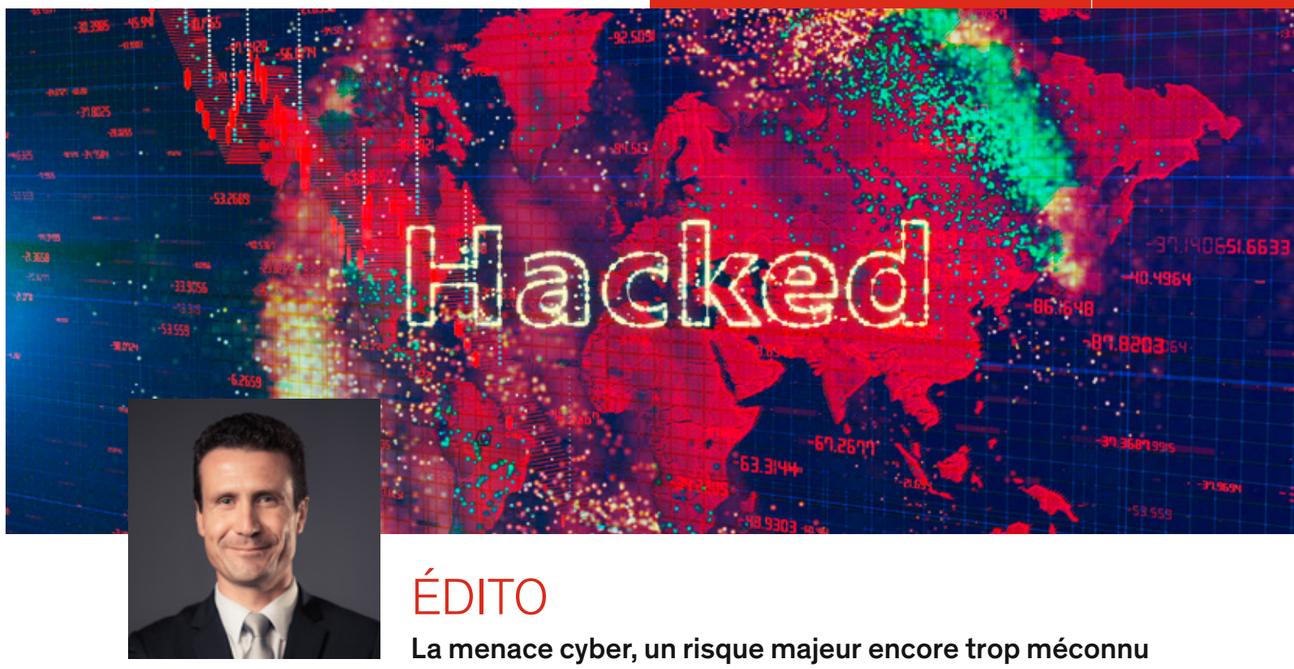
SWISS RISK & CARE
Our independence ▪ Your best insurance

INSURANCE INSIDE
N° 25
MARS 2022



ÉDITO

La menace cyber, un risque majeur encore trop méconnu

2022 sera-t-elle l'année qui marquera la fin de la pandémie ? Au moment où, à l'instar de plusieurs pays en Europe, le Conseil fédéral lève les mesures de lutte contre le virus, l'espoir d'un retour à la normalité se profile. Espérons pour nos entreprises comme pour nos vies personnelles que ce retour s'inscrive dans le long terme.

Si la crise sanitaire s'éloigne, la menace cyber ne cesse, quant à elle, de croitre. La guerre qui vient de se déclarer en Ukraine est également digitale et s'accompagne d'une multiplication des attaques cyber. Désormais, la crainte d'une pandémie numérique c'est-à-dire l'attaque simultanée de plusieurs entreprises à plusieurs endroits de la planète dans le but de provoquer une paralysie de l'économie mondiale, s'intensifie.

Toutes les entreprises sont concernées quel que soit le secteur. Les grandes entreprises et les multinationales ont compris que le risque cyber n'était pas uniquement l'affaire du département informatique mais qu'il s'agissait aujourd'hui d'une urgence absolue dont la responsabilité relevait des directions et des conseils d'administration. À l'inverse, les PME sous-estiment trop souvent leur exposition au risque et n'investissent pas assez dans leur sécurité. Moins bien armées à la fois pour prévenir le risque et pour réagir rapidement et efficacement à une attaque, elles se retrouvent les cibles de plus en plus fréquentes des pirates. Avec parfois des conséquences dramatiques sur leur activité.

Dans ce contexte, l'assurance cyber constitue-t-elle une solution ? Oui, indubitablement, mais encore faut-il comprendre ce que couvre cette assurance, quelles sont les conditions pour pouvoir y souscrire. C'est ce que nous vous proposons de découvrir dans les pages qui suivent.

Je profite de cette tribune pour vous partager ma fierté de devenir le nouveau Directeur général de Swiss Risk & Care. Je souhaite inscrire mon action dans celle que nous menons depuis plusieurs années et qui a privilégié l'investissement dans la digitalisation et la sécurité informatique pour renforcer le service et la proximité auprès de nos clients.

Bonne lecture !

David Cochet
Directeur général

L'INTERVIEW

Le risque cyber, l'affaire de tous dans l'entreprise

Marie de Fréminville est experte en gouvernance et en gestion du risque. Après un parcours au sein de grandes entreprises internationales, elle met son expérience au service des entreprises suisses au sein de son cabinet de conseil Starboard Advisory. Par ailleurs, elle est Vice-Présidente du Cercle suisse des administratrices.

Le risque cyber est-il bien pris en compte par les entreprises ?
La plupart des PME minimisent le risque cyber. Pourtant, elles ne sont pas à l'abri des attaques. Pour les cybercriminels, il est plus facile de pirater des PME, qui manquent de ressources dédiées, et d'obtenir le paiement d'une rançon. Par ailleurs, elles sont la porte d'entrée pour atteindre leurs clients, avec lesquels elles sont connectées.

Le risque cyber n'est pas qu'un sujet IT. C'est aussi une responsabilité des dirigeants. Comment les sensibiliser ?
Les dirigeants sont responsables de la pérennité de l'entreprise. Une cyberattaque peut avoir des impacts graves, en termes financiers et de réputation. La faille étant à 95 % humaine, la formation de tous est indispensable. Les outils IT sont nécessaires, mais ne suffisent pas : les dirigeants doivent identifier les actifs critiques à protéger, mettre en place une organisation, des processus, des règles, un audit régulier, et se préparer à gérer la crise qui va arriver.

Quels sont les enjeux à venir de la cyber sécurité ?
Les attaques vont se multiplier. La cybersécurité est basée sur la gestion de risques, l'anticipation de la crise, la mise en place de moyens, notamment humains, le développement d'une culture dans l'ensemble des organisations (le risque est systémique !). Comme pour l'automobile, la sécurité s'améliorera avec du matériel fiable, des contrôles techniques, un permis de conduire obtenu grâce à de la formation, un code de la route et un contrôle de l'application de règles standard.

Dirigeants, membres de CA, une responsabilité de plus en plus exposée

Vous êtes membres de la direction de l'entreprise ou de son conseil d'administration… Savez-vous que votre responsabilité civile personnelle peut être engagée dans l'exercice de votre fonction ? En cas de condamnation, vous serez redevables sur vos biens propres. Les raisons pour lesquelles vous pouvez être mis en cause sont multiples, tout comme vos détracteurs qui peuvent être les actionnaires, l'entreprise elle-même, les autorités réglementaires, des créanciers, des concurrents, des clients ou vos employés. Des solutions existent pour vous protéger. Nous vous proposons de les découvrir en visionnant le webinaire que nous avons organisé le 9 mars dernier et qui a réuni juristes, experts en responsabilités des dirigeants, en cyber sécurité et en gouvernance.

Revoir le replay de notre webinaire :
https://www.swissriskcare.ch
rubrique « Nous connaitre/Nos webinaires »

Participez à notre enquête de lectorat

Vous êtes lecteur d'Insurance Inside ?

Votre avis nous intéresse !

Merci de prendre 5 minutes pour répondre à ces quelques questions à découvrir en flashant le QR Code.

Impressum
Éditeur : Swiss Risk & Care - insurance-inside@swissriskcare.ch - T +41 58 178 85 85 • Directeur de Publication : David Cochet • Responsable Éditoriale : Valérie Cruchet
Impression : Imprimerie Baudat, L'Orient • Crédit photo : Swiss Risk & Care, iStock by Getty, Céline Michel, studioregard.ch.

SWISS RISK & CARE
Our Independence • Your best Insurance

Qu'est-ce qu'une assurance cyber et faut-il la souscrire ?

Il ne se passe pas un jour sans qu'une entreprise, petite ou grande, ne soit victime d'une attaque cyber. Pour les organisations, la question n'est plus de savoir si elles vont en être victimes mais quand. Face à cette situation, comment les assureurs couvrent-ils ce risque ? Etat des lieux.

L'assurance cyber constitue la solution ultime une fois que l'entreprise a déployé toutes les mesures de prévention pour protéger ses données numériques, sécuriser son environnement informatique et se conformer à la règlementation en vigueur. *« Sans ce travail préalable, et les investissements indispensables qui en découlent, il sera difficile pour une entreprise de s'assurer »*, explique Sophie Di Meglio, Directrice des Risques spéciaux chez Swiss Risk & Care.

Ce que couvre une assurance cyber

L'assurance cyber s'applique en cas d'incident de sécurité et d'atteintes au système d'information ou aux données personnelles et confidentielles d'une entreprise. Elle offre principalement :

- **L'assistance et la gestion de la crise :** l'assureur met à la disposition de l'entreprise une hotline 24h/7j qui va l'orienter vers des spécialistes IT, des experts en gestion de crise et des juristes. Ce service mobilisable aux premières heures de l'attaque est déterminant dans la gestion de la crise afin d'en limiter l'impact, notamment sur la réputation de l'entreprise.

- **La garantie dommages propres :** elle couvre notamment les coûts engagés pour permettre la restauration des données, la décontamination des systèmes, les frais de notification aux autorités et tiers, de monitoring et de surveillance ainsi que la perte de revenus consécutive à une interruption d'exploitation (avec un délai de carence entre 6h et 48h selon l'assureur). Sont également pris en charge les frais relatifs à la cyber extorsion, tels que le coût des consultants mobilisés afin d'éviter que la menace de blocage ou de vols de données ne soit exécutée. Certains assureurs acceptent encore de payer la rançon en l'absence d'aucune autre alternative mais c'est de plus en plus rare.
Cette garantie devrait pouvoir s'étendre aux prestataires du preneur d'assurance qui gèrent son système informatique ou hébergent ses données, en cas d'incidents.

- **La garantie responsabilité civile :** elle prend en charge les frais de défense et les dommages-intérêts éventuels dans le cadre de réclamations de tiers liées à la protection des données ou en cas d'atteinte dans le cadre de diffusion de contenu électronique.

« Les critères et les conditions des assureurs évoluent dans le temps, en particulier en raison de la hausse exponentielle du nombre des attaques cyber depuis 2 ans. »

Chiffres clés

1 attaque toutes les 39 secondes

6'000 milliards de $ estimés **pour le coût des attaques** (soit plus élevé que le PIB du Japon) **en 2021**

+ 400 % d'attaques en 2020

+ de 1'000 milliards de $ dépensés en cybersécurité en 2021

Certains assureurs proposent une extension cyber à leur police d'assurance Choses ou Responsabilité civile mais les garanties sont généralement moindres et les compensations financières faibles. *« Néanmoins, c'est une solution intéressante pour les PME*, précise Sophie Di Meglio, *les compagnies pionnières de l'assurance Cyber étant aujourd'hui plus exigeantes pour les assurer voire, pour certaines, n'assurant plus les PME en deçà d'un certain chiffre d'affaires. »*

Et ce qu'elle ne couvre pas

Parmi les principales exclusions, nous trouvons les dommages corporels, matériels et de préjudices de fortune, les dommages dus à l'usure ou au vieillissement des supports de données ou au manque de compatibilité entre données numériques et logiciels ou entre logiciels, la défaillance ou panne d'infrastructures d'utilité publique (interruption de réseau), la violation de brevets commerciaux, etc. D'un assureur à l'autre, les obligations imposées au preneur d'assurance diffèrent et pourraient le priver de garantie en cas de non-respect.

Et Sophie Di Meglio de rappeler : *« Il est important de lire l'intégralité des contrats ce qui peut être complexe pour un néophyte. Se faire accompagner par un courtier constitue la bonne solution d'autant que les critères et les conditions des assureurs évoluent dans le temps, en particulier en raison de la hausse exponentielle du nombre des cyber attaques depuis 2 ans. »*

Ne seront également pas couverts les dépenses consécutives aux nouveautés introduites à la suite d'un sinistre (par exemple, l'actualisation de logiciels ou du système IT), les frais et pertes liés à un manque de capitaux causé par un sinistre assuré, et ce qui relève d'un contrat Responsabilité Civile des Dirigeants.

Sophie Di Meglio ajoute : *« certains secteurs professionnels considérés comme très exposés au risque cyber sont de fait exclus par les assureurs. C'est le cas des entreprises qui réalisent la majorité de leur chiffre d'affaires sur internet, des prestataires IT, des infrastructures « critiques » telles que les sociétés de télécom, les établissements médicaux ou les fournisseurs d'eau, etc. »*

Ce que vous demandera un assureur

Généralement, l'entreprise devra renseigner un questionnaire de souscription. Certaines compagnies n'en exigeront pas s'il s'agit de l'extension d'un contrat Choses ou RC existant.

Pour accepter d'assurer l'entreprise, les compagnies portent une attention particulière à plusieurs points tels que la formation régulière du personnel sur la protection des données et la sécurité, le profil et la quantité de données sensibles traitées, la régularité des mises à jour, la protection contre les malwares, la sécurité du réseau et l'authentification multi-facteur, la sauvegarde et la restauration des données, le plan de réponse et les tests de ce dernier.

Attention : un seul incident survenu par le passé peut suffire à rendre l'entreprise difficilement éligible à une assurance cyber !

L'assurance cyber, une aide à la prévention

Protéger ses données doit constituer la priorité des conseils d'administration et des comités de direction. Ils pourraient se voir reprocher une absence ou une insuffisance de gestion des risques cyber (en référence aux articles 717 et 754 du Code des Obligations). L'assurance Cyber constitue un outil de prévention efficace. Les conditions exigées par les assureurs pour la souscription sont finalement les mesures que toute entreprise devrait aujourd'hui avoir mises en place pour lutter efficacement contre les attaques cyber.