KESSLER

Cyber Message 2026

Risk and Insurance



EN AVANT, SEREINEMENT.

Cyber Message 2026

Le sujet de la cybersécurité va bien au-delà de la simple maîtrise des risques informatiques. Les entreprises peuvent être attaquées via leurs prestataires de services, subir des dommages résultant de la combinaison de tromperie et de technologie, tandis que l'intelligence artificielle (IA) fait émerger de nouvelles questions en matière de responsabilité. Longtemps centrée sur la prévention et la défense technique, la gestion des risques englobe désormais aussi la préparation aux situations de crise et la capacité à y répondre. Dix ans d'expérience en matière de cybersécurité chez Kessler nous montrent que les choses se compliquent là où la conduite d'entreprise, la responsabilité civile et l'assurance se croisent – et lorsque les responsabilités, les processus et les couvertures n'ont pas été coordonnés en amont.

Changements juridiques

LA CYBERGOUVERNANCE – UNE MISSION DE DIRECTION

La cybersécurité ne relève plus du seul domaine informatique mais constitue un véritable enjeu stratégique et réglementaire pour la direction. Au titre de leurs obligations légales de diligence et de surveillance, le conseil d'administration et la direction doivent également intégrer les cyberrisques dans l'exercice de leurs responsabilités. Les cyberrisques doivent faire partie intégrante de la gouvernance d'entreprise, de la gestion des risques et des décisions stratégiques, notamment lors de l'externalisation de certaines activités ou dans le cadre d'opérations de fusion-acquisition. Cela implique des responsabilités clairement définies, un reporting régulier, une surveillance adéquate et une gestion des risques résiduels bien réfléchie.

Il s'agit d'examiner tout transfert éventuel de cyberrisques et de documenter les décisions. Lorsqu'un manquement aux devoirs de diligence ou de surveillance cause un préjudice, la responsabilité personnelle des membres des organes dirigeants peut être engagée. Une assurance responsabilité civile des dirigeants (D&O) peut contribuer à couvrir certaines conséquences financières d'une mise en cause, mais elle ne saurait se substituer aux obligations légales des membres du conseil d'administration et de la direction.

RESPONSABILITÉ : ENTRE ENGAGEMENTS CONTRACTUELS ET ATTENTES DES CLIENTS

Les clients n'attendent plus seulement des produits et des services fiables mais exigent des engagements contractuels garantissant la sécurité, la disponibilité et la continuité des composants numériques, des données et des systèmes. Un vrai dilemme pour les prestataires : plus les accords de niveau de service (SLA) sont détaillés, plus ils deviennent une référence pour déterminer l'étendue de leur responsabilité en cas de litige. Des engagements trop ambitieux peuvent exposer les prestataires à des risques qu'ils ne sont pas en mesure de maîtriser, tant sur le plan technique qu'organisationnel et qui, parfois, ne peuvent être transférés à l'assurance que de manière limitée. L'assurance responsabilité civile couvre en principe les conséquences de la responsabilité légale, mais pas nécessairement celles d'engagements contractuels supplémentaires. Il est donc essentiel de trouver un équilibre entre les attentes des clients et les capacités réelles du prestataire. Une répartition claire des risques, des engagements réalistes et des limites de responsabilité précises sont donc essentiels.

IA – NOUVEAU FACTEUR DE RISQUE

Un agent d'IA supprime involontairement des données de production, un chatbot fait une promesse erronée, ou un outil d'IA traite de manière inadéquate des données à caractère personnel : l'IA peut amplifier les risques existants. Elle facilite les cyberattaques, rend les tentatives de phishing plus crédibles, favorise les violations de la protection des données ou génère des résultats erronés. Selon la nature du sinistre, différentes assurances sont concernées : la cyber en cas d'incidents de sécurité ou de violation de données, la RC professionnelle en cas de conseil erroné ou de prestations IT défaillantes, l'assurance contre les abus de confiance en cas de paiements frauduleux liés à l'IA, ou la « D&O » lors d'enjeux de gouvernance. La question n'est pas tant de savoir si l'IA est « assurée », mais plutôt de vérifier que les polices existantes couvrent les risques découlant de ses usages concrets.

Risques actuels

RISQUES TECHNOLOGIQUES POUR LES ENTREPRISES INDUSTRIELLES

De nombreuses entreprises industrielles sont aujourd'hui aussi des entreprises technologiques qui développent des logiciels, exploitent des plateformes numériques ou enrichissent leurs machines en services connectés, tels que la maintenance à distance ou les modèles « Software-as-a-Service ».

Les frontières entre responsabilité civile produits, responsabilité civile professionnelle et cyberresponsabilité deviennent de plus en plus floues et complexes. Ce qui constituait autrefois un dommage mécanique peut désormais résulter d'une défaillance logicielle, d'une violation de données à caractère personnel ou encore d'un préjudice purement financier. Les couvertures traditionnelles de responsabilité civile d'entreprise et de responsabilité civile produits ne sont pas toujours conçues pour répondre à ces nouveaux scénarios. Il est essentiel pour les entreprises industrielles d'identifier leurs prestations numériques et d'intégrer les risques associés dans leur gestion des risques.

Pour les entreprises actives à l'international, le nouveau cadre européen en matière de responsabilité du fait des produits renforce les risques. Dès le 9 décembre 2026, les logiciels pourront, sous certaines conditions, relever de la notion de produit. Des défauts de logiciel, ou des mises à jour insuffisantes pourront ainsi entrer dans le champ de la responsabilité du fait des produits.

SCÉNARIO DE CYBERCRIMINALITÉ

« Veuillez effectuer de toute urgence un virement bancaire de CHF 500 000. » Le message semble provenir du CEO, le collaborateur procède au transfert. Mais l'ordre est un faux et l'argent se volatilise. Comment couvrir ce préjudice ?

Dans la gestion des sinistres, ce type de fraude peut prendre différentes formes : piratage d'un compte de messagerie, vol d'identifiants ou encore manipulation de coordonnées bancaires. Pour l'entreprise, il s'agit d'un même incident de cybercriminalité. Du point de vue de l'assurance, en revanche, c'est le mécanisme précis du sinistre qui détermine les couvertures susceptibles d'intervenir. Les frais consécutifs à l'incident, tels que l'expertise forensique, l'analyse du système compromis ou sa remise en état, peuvent relever de l'assurance cyber. En revanche, la perte résultant du virement frauduleux relève plutôt de l'assurance contre les abus de confiance, sous réserve des conditions, sous-limites et obligations de vérification prévues par le contrat. Selon les circonstances et les dispositions de la police, un même incident peut ainsi être couvert en totalité, en partie, ou pas du tout.

L'enjeu ne réside donc pas dans le choix des polices d'assurance, mais dans l'analyse préalable des scénarios de cybercriminalité et de leur couverture. Une approche fondée sur des garanties isolées, sans analyse des processus internes ni vérification des obligations contractuelles, peut laisser subsister des lacunes importantes au moment du sinistre.

Incidents cyber

LES FACTEURS DE COÛTS CACHÉS

Les cyberincidents coûtent cher, mais selon notre expérience, ils donnent rarement lieu, en Suisse, à des demandes de dommages-intérêts du fait des obstacles juridiques importants ; il faut prouver la faute, le lien de causalité et un préjudice patrimonial concret. Dans notre portefeuille cyber, les indemnités de dommages-intérêts représentent moins de 5 % des paiements, y compris la défense contre les prétentions injustifiées. Les coûts portent sur la réponse aux incidents, le forensique, la restauration, les interruptions d'activité, les obligations de déclaration et les exigences réglementaires, avec des conséquences financières, opérationnelles et réputationnelles.

Pour les entreprises opérant à l'international, cela ne suffit pas. Selon la juridiction concernée, le risque de responsabilité est plus élevé : dans l'UE, le RGPD prévoit des amendes et des demandes de dommages-intérêts, tandis qu'aux États-Unis, des recours collectifs et des dommages-intérêts punitifs sont à prévoir. Ce n'est donc pas seulement le siège social de l'entreprise qui est déterminant, mais aussi la localisation des clients, des filiales ou des données à caractère personnel.

CYBERATTAQUES CONTRE LES PRESTATAIRES DE SERVICES INFORMATIQUES

Les prestataires IT assurent la continuité des activités de leurs clients. Lorsque ceux-là sont victimes d'une cyberattaque, les conséquences touchent souvent de nombreux clients simultanément : interruptions d'activité, fuites de données et coûts de migration. Le cas d'Unico Data illustre bien l'ampleur du phénomène : après une attaque par ransomware en 2023, de nom-

breux clients se sont retrouvés simultanément hors ligne. Fin 2025, l'entreprise a cessé ses activités – non pas en raison de coûts immédiats s'élevant à plus de CHF 1 million, mais à cause de l'atteinte à sa réputation et de la perte de clients.

Qui supporte un tel préjudice ? Les contrats limitent souvent les droits à indemnisation aux dommages directs, tandis que les coûts induits et les pertes de chiffre d'affaires ne sont couverts que dans une mesure limitée. Si le prestataire de services fait défaut ou cesse son activité, les recours contractuels restent sans effet. La cyberassurance couvre généralement les propres dommages, et non ceux des clients.

La protection commence au sein-même de l'entreprise : les contrats d'externalisation, les limites de responsabilité, la couverture cyber et les plans de continuité des activités doivent être régulièrement vérifiés. Car lorsqu'on externalise des services IT, on confie ses systèmes à un tiers, mais pas le risque.

Kessler – depuis 10 ans à vos côtés face aux cyberrisques

Depuis le placement de la première cyberassurance par Kessler en 2016, le marché a profondément évolué. Dès 2020, une phase de durcissement s'est installée, marquée par des sinistres importants, des capacités limitées et des exigences croissantes en matière de cybersécurité. Aujourd'hui, le marché s'est détendu. Des capacités supplémentaires et une concurrence intense créent de nouvelles opportunités de placement. Le contexte reste toutefois exigeant en raison des attaques basées sur l'IA, des risques liés à la chaîne d'approvisionnement et d'une réglementation croissante.

Des normes de sécurité rigoureuses, une communication claire sur les risques et une prévention efficace des sinistres restent les éléments-clé d'une couverture optimale.

Nos spécialistes cyber vous proposent un accompagnement complet, en collaboration avec notre partenaire Marsh si nécessaire, allant des autoévaluations et des analyses de maturité jusqu'à la gestion des sinistres. De plus, nous avons développé pour les PME une solution très attractive de contrat-cadre adaptée à leurs besoins spécifiques. En 2026, nous avons pu placer la solution « cyber blue line » pour trois années supplémentaires. Notre objectif reste la même : identifier les risques à un stade précoce, renforcer la résilience et accompagner nos clients de manière fiable en cas d'incident.

KESSLER EN BREF

Kessler est l'entreprise leader dans le domaine du conseil global en risques, assurances et prévoyance en Suisse. Nous nous occupons de plus de 1 600 moyennes et grandes entreprises suisses issues des services, du commerce et de l'industrie ainsi que du secteur public. Grâce à nos compétences dans les différents secteurs économiques, à nos collaborateurs qualifiés et à notre position de leader sur le marché, nous contribuons de manière significative au succès durable de nos clients. En tant que partenaire fiable, nous suscitons leur enthousiasme et leur ouvrons de nouvelles perspectives par notre gestion sûre des risques. Fondée en 1915, Kessler compte aujourd'hui 390 collaborateurs travaillant au siège à Zurich et sur les sites de Bâle, Berne, Genève, Lausanne, Lucerne, Neuchâtel, Saint-Gall, Sion et Vaduz. En tant que partenaire suisse de Marsh, nous faisons depuis 1998 partie d'un réseau de spécialistes issus de toutes les branches de gestion des risques et disposons d'une grande expérience dans le suivi des programmes d'assurances globaux. Marsh est un leader mondial de services professionnels en risques, réassurance, ressources humaines et investissements, ainsi que du conseil en stratégie, accompagnant des clients implantés dans 130 pays avec plus de 90 000 collaborateurs (NYSE : MRSH).

Vous trouverez de plus amples informations sur www.kessler.ch, www.marsh.com et www.corporate.marsh.com.

KESSLER & CO SA
Forchstrasse 95
Case Postale
CH-8032 Zurich
T +41 44 387 87 11
www.kessler.ch