KESSLER

Cyber Message 2025

Risk and Insurance

EN AVANT, SEREINEMENT.

Les tensions géopolitiques, la guerre hybride et les attaques alimentées par l'intelligence artificielle façonnent l'environnement mondial 2025 des cyberrisques. La Suisse n'y échappe pas. De nouvelles obligations de déclaration en cas d'incident cyber visent à renforcer de manière proactive la protection des entreprises et des autorités. Mais quels sont les domaines touchés ? Kessler partage son expérience afin de mettre en lumière l'importance de ces enjeux pour la sécurité des entreprises. L'intégration de ces enseignements dans la gestion des risques constitue un levier essentiel pour renforcer durablement la résilience.

Changements juridiques

OBLIGATION DE DÉCLARATION POUR LES EXPLOITANTS D'INFRASTRUCTURES CRITIQUES

Depuis le 1er avril 2025, la Suisse impose aux exploitants d'infrastructures critiques de déclarer tout incident cyber. Les secteurs concernés sont notamment l'énergie, les transports, la santé, la finance et les administrations publiques. Toute cyberattaque doit être signalée dans un délai de 24 heures à l'Office fédéral de la cybersécurité (OFCS) dès lors que la stabilité de l'infrastructure est affectée, que des données sont exfiltrées ou qu'il y a chantage ou extorsion. Depuis le 1er octobre 2025, un défaut de déclaration expose les organismes et autorités concernés à des amendes pouvant atteindre CHF 100 000. Cette obligation découle de la révision de la Loi sur la sécurité de l'information (LSI), qui vise à renforcer la résilience des infrastructures critiques.

INTELLIGENCE ARTIFICIELLE

Les agents d'IA accélèrent les processus et optimisent les décisions, mais comportent également des cyberrisques majeurs. Données d'entraînement manipulées, responsabilités floues et actions incontrôlées augmentent le potentiel d'abus. Le AI Act européen, adopté en 2024, fixe des règles claires : les agents d'IA utilisés dans des domaines sensibles comme l'évaluation de la solvabilité ou la gestion du personnel sont classés comme systèmes à haut risque et soumis à des exigences strictes en matière de transparence, de contrôle et de gestion des risques. Les fournisseurs de modèles génératifs doivent en outre respecter des obligations supplémentaires en matière de fiabilité et de traçabilité, applicables aussi aux entreprises suisses en lien avec l'UE.

Certains acteurs dénoncent des freins à l'innovation, tandis que les multinationales mettent en garde contre la complexité réglementaire et les coûts élevés, réclamant des directives plus précises et des délais de transition prolongés. Parallèlement, des codes de conduite et standards volontaires (p. ex. CEN, ETSI) émergent. La Suisse prévoit d'ici 2026 un cadre légal propre, inspiré de celui de l'UE. L'accent est mis sur les agents d'IA agissant de manière autonome ou en interaction avec les clients. Leur exploitation exige expertise technique et anticipation réglementaire : gestion des risques, processus transparents et contrôles internes deviennent à la fois une obligation et un avantage concurrentiel.

Risques actuels

CYBERSÉCURITÉ DANS LE CADRE DES OPÉRATIONS DE FUSION-ACQUISITION

La cybersécurité est encore trop négligée lors des fusions-acquisitions. Selon IBM, plus de la moitié des entreprises n'évaluent les cyberrisques qu'après la due diligence. Or, il est essentiel d'identifier et de quantifier ces risques en amont par une analyse de l'infrastructure de la cible et une évaluation continue des impacts business tout au long du cycle de transaction. C'est la seule manière de sécuriser les rendements et protéger durablement la valeur. En partenariat avec Marsh, Kessler identifie la vulnérabilité de la cible à l'échelle mondiale et évalue les conséquences financières de pannes, de violations de données et d'attaques par rançongiciels. Les résultats sont présentés dans un rapport structuré, assorti de recommandations hiérarchisées en fonction des priorités sur les mesures ayant un impact significatif sur la valeur de la transaction.

GESTION DE CRISE – SÉCURITÉ EN PÉRIODE DIFFICILE

Les cyberassurances offrent bien plus qu'une sécurité financière : elles garantissent un véritable dispositif de gestion de crise, permettant de réagir rapidement et efficacement aux incidents de sécurité. Cela inclut des procédures de réponse aux incidents (détection, analyse, confinement), la conformité légale des déclarations ainsi qu'un plan de continuité d'activités (Business Continuity Plan – BCP) pour sécuriser les processus critiques. Des experts forensiques, des spécialistes en relations publiques et en droit travaillent 24h/24 à l'analyse, au confinement et à la restauration des systèmes. Kessler vous accompagne depuis la déclaration du sinistre jusqu'à la coordination avec les prestataires et la présentation des rapports aux assureurs.

CYBERRISQUES DANS LE CADRE DE SPIN-OFFS

Lors de la cession d'une société (spin-off), le vendeur propose bien souvent la mise à disposition de l'infrastructure IT pour une période transitoire de 6 à 36 mois, encadrée par un accord de services de transition (Transition Service Agreement – TSA). Or, les cyberassurances classiques ne couvrent pas cette phase : en cas d'incident ou d'attaque, les risques de responsabilité sont importants. La solution passe par une assurance responsabilité civile professionnelle (Professional Indemnity – PI), qui couvre les erreurs ou omissions dans la prestation de service et comble ainsi la lacune de couverture liée aux scénarios informatiques transitoires.

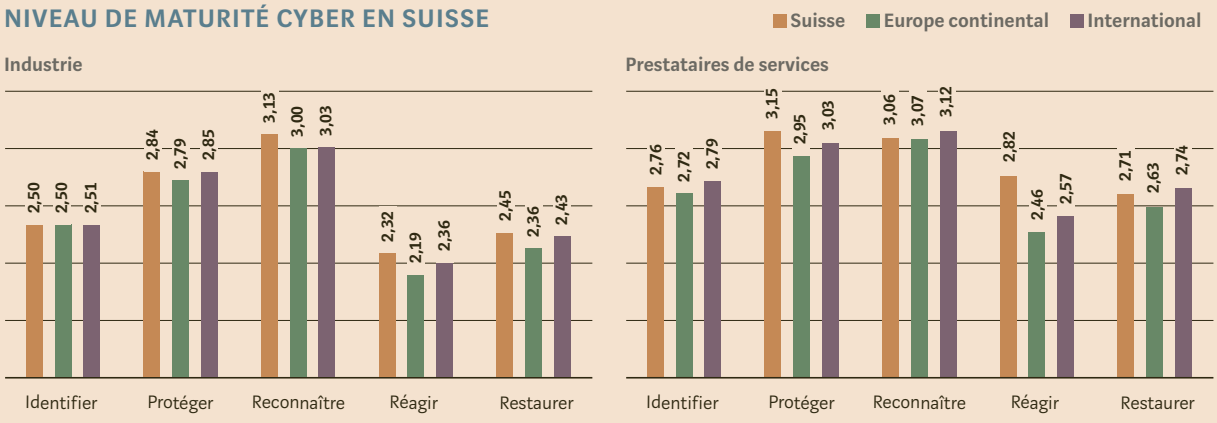
NIVEAU DE MATURITÉ CYBER EN SUISSE : OÙ EN SONT LES ENTREPRISES ?

Depuis début 2024, Kessler utilise l'outil d'autoévaluation cyber (Cyber Self Assessment Tool – CSA) de Marsh, combiné au référentiel de cybersécurité du NIST (National institute of standards and technology), pour évaluer la résilience cyber des clients (niveau 1 = partiellement mis en œuvre à niveau 4 = adaptatif). Les entreprises industrielles en Suisse obtiennent en moyenne 2,71. Les prestataires de services (IT, finance, conseil) atteignent 2,91. Ces résultats sont supérieurs aux moyennes européennes et internationales. L'avance des prestataires de services est particulièrement marquée dans les domaines « Protéger » (+0,20) et « Réagir » (+0,36). La rapidité de réaction aux incidents s'avère en effet décisive pour limiter les dommages.

CHAÎNE D'APPROVISIONNEMENT – ENSEIGNEMENTS

Les prestataires informatiques sont essentiels pour la plupart des entreprises, mais aussi une cible privilégiée des attaquants. Près d'un tiers des cyberincidents leur sont imputables, principalement en raison de configurations défaillantes, de comptes non sécurisés ou de mises à jour tardives. Chaque entreprise doit donc intégrer systématiquement ses prestataires IT dans sa gestion des risques, les auditer régulièrement et veiller à ce que les cyberassurances couvrent également les incidents liés à la sous-traitance. On ne peut pas externaliser la responsabilité, mais on peut transférer les risques.

NIVEAU DE MATURITÉ CYBER EN SUISSE



Marché de la cyberassurance

NÉGOCIATIONS DE RANÇON

Le chantage est un élément clé du fonctionnement du « ransomware-as-a-service » et consiste à exiger une rançon pour déverrouiller des données cryptées ou empêcher leur publication. Souvent, les entreprises paient, à défaut d'alternative. Les cyberassurances ne couvrent la rançon que partiellement, et en dernier recours.

Dans l'idéal, les négociations sont menées par des experts en gestion de crise qui gèrent la communication et les tractations, vérifient la crédibilité des demandes et tentent de réduire le montant de la rançon. L'objectif est de récupérer les données, d'obtenir la garantie de non-récidive et de communiquer le mode opératoire des criminels. De plus, ils formulent des recommandations pour prévenir de futures attaques.

CYBERATTAQUES EN 2024 : PLUS DE DÉCLARATIONS, MOINS DE DOMMAGES

Selon le Marsh Claims Report, les sinistres déclarés par les preneurs d'assurance cyber en Europe ont augmenté de 61 % en 2024. En même temps, la résistance croissante et la vitesse de réaction ont limité leurs impacts. Les perturbations de la chaîne d'approvisionnement numérique, comme la panne mondiale de CrowdStrike, ont été des déclencheurs importants. La part des attaques par rançongiciels a chuté, passant d'un pic de plus de 40 % en 2021 à 18 % en 2024, tandis que les attaques de phishing dopées par l'intelligence artificielle ont progressé. Il est frappant de constater que l'authentification multifactorielle (MFA) reste le dispositif de sécurité le plus souvent compromis.

KESSLER EN BREF

Kessler est l'entreprise leader dans le domaine du conseil en risques, assurances et prévoyance en Suisse. Nous nous occupons de plus de 1 500 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 370 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. Actif dans plus de 130 pays, Marsh est le principal courtier en assurances et conseiller en gestion des risques sur le plan mondial et fait partie de Marsh McLennan (NYSE : MMC).

Vous trouverez de plus amples informations, sous www.kessler.ch, www.marsh.com et www.mmc.com.

KESSLER & CO SA
Avenue de la Gare 44
Case Postale 950
CH-1001 Lausanne
T: +41 21 321 60 30
www.kessler.ch

Marsh Network