KESSLER

CYBER RISK & INSURANCE
3E ÉDITION MISE À JOUR (2021)

EN AVANT, SEREINEMENT.

	AVANT-PROPOS	5
1	VOTRE PARTENAIRE DE CONFIANCE	6
2	CYBERRISQUES	9
	2.1 RÉPERCUSSIONS FINANCIÈRES	11
	2.2 RISQUE DE LA CHAÎNE D'APPROVISIONNEMENT IT: QUI LE SUPERVISE?	12
3	GOUVERNANCE D'ENTREPRISE	14
	3.1 OBLIGATIONS DU CONSEIL D'ADMINISTRATION	14
	3.2 L'IMPORTANCE DE LA DÉCISION DÉLIBÉRÉE	16
4	PROTECTION ET SÉCURITÉ DES DONNÉES: QUEL RAPPORT AVEC LE CYBERRISQUE?	18
	4.1 LA SUISSE ET L'INFLUENCE DE L'UE: QUESTIONS À L'AGENDA D'ICI 2022	19
	4.2 OBLIGATIONS DE NOTIFICATION: COMPARAISON SUISSE VS UE	20
	4.3 UN PLAN D'ACTION SUR MESURE VERS LA CONFORMITÉ À LA LPD: LES FONDAMENTAUX	22
	4.4 LISTE DES AMENDES DANS LA LPD RÉVISÉE	23
	4.5 EXCURSUS: LOIS SUR LA PROTECTION DES DONNÉES AUX ÉTATS-UNIS	24
5	ASSURABILITÉ DES CYBERRISQUES	25
	5.1 CYBERASSURANCES: DOMMAGES ASSURABLES	26
	5.2 ASSURANCE CONTRE LES ABUS DE CONFIANCE	28
	5.3 ASSURANCE CHOSES ET PERTE D'EXPLOITATION, ASSURANCE TECHNIQUE	29
6	DU CYBERINCIDENT AU SINISTRE COUVERT PAR LA CYBERASSURANCE	30
7	LE PROCESSUS EN DEUX PHASES	32
	7.1 PREMIÈRE PHASE: DIALOGUE SUR LES CYBERRISQUES	32
	7.2 DEUXIÈME PHASE: DEMANDE D'OFFRES FERMES	32

AVANT-PROPOS

Il y a (seulement) cinq ans, le travail des spécialistes du conseil était centré sur la question: «Que peut-il arriver concrètement?».

Aujourd'hui, plusieurs centaines d'entretiens avec des interlocuteurs d'entreprises suisses nous permettent d'affirmer que les organes de décision sont très conscients des cyberrisques. Les scénarios sont connus, les entreprises ont quantifié leurs cyberrisques et se sont assurées contre les problèmes. En collaboration avec les assureurs, nous avons amélioré sans relâche les produits proposés. Assureurs et courtiers savent désormais régler toutes sortes de sinistres. Cette montée en compétences nous a parfois demandé d'importants efforts à tous. En résumé, nous pouvons dire que les entreprises suisses sont devenues plus solides et surtout, qu'elles sont préparées à toute éventualité.

Pascal Schweingruber
Membre du Comité de direction

Lors de la session d'automne 2020, les deux chambres fédérales ont adopté la nouvelle loi suisse sur la protection des données. Nous saisissons cette occasion pour publier la troisième édition mise à jour de la brochure Cyber Risk & Insurance, où nous analysons les nouveaux aspects juridiques et proposons notre expérience de la gestion des cyberrisques.

Je remercie sincèrement toutes les personnes qui ont contribué à cette édition et l'ont enrichie de leur expertise: Simon Künzler (conseil en risques), Melanie Koller (juridique), Nadine Janser (risques spéciaux), Simon Holtz (assurance de choses) et Patrick Dummermuth (Claims Advocacy).

Je vous souhaite une lecture instructive.

1
VOTRE PARTENAIRE DE CONFIANCE

Nous vous aidons à créer un cyberdispositif qui permet à votre organisation de renforcer sa capacité de résistance face aux cyberattaques. Pour atteindre cet objectif, nous adoptons une approche globale et personnalisée et faisons appel à nos compétences spécifiques et méthodiques axées sur la pratique.

SITUATION INITIALE ET EXPOSITION AU RISQUE

Les cyberattaques sont en constante évolution. Elles se développent dans des chaînes d'approvisionnement, des infrastructures d'information et de communication interconnectées, complexes et dynamiques, dans l'«Internet of Things», respectivement «every thing», et en particulier dans la manipulation inconsidérée des e-mails et d'Internet par des collaborateurs. D'un côté, les innovations et les développements numériques tels que l'industrie 4.0 ont offert aux organisations d'énormes opportunités de croissance et de rationalisation. D'un autre côté, elles ont aussi entraîné une augmentation considérable des risques potentiels. D'une manière générale, un manquement dans le domaine de la cyberrésilience (capacité de résistance) peut compromettre la gouvernance d'entreprise et entraîner de graves répercussions financières et non-financières. Cette situation initiale montre que l'ensemble des cyberrisques doit être entièrement analysé, évalué et finalement contenu au moyen de mesures préventives et réactives appropriées.

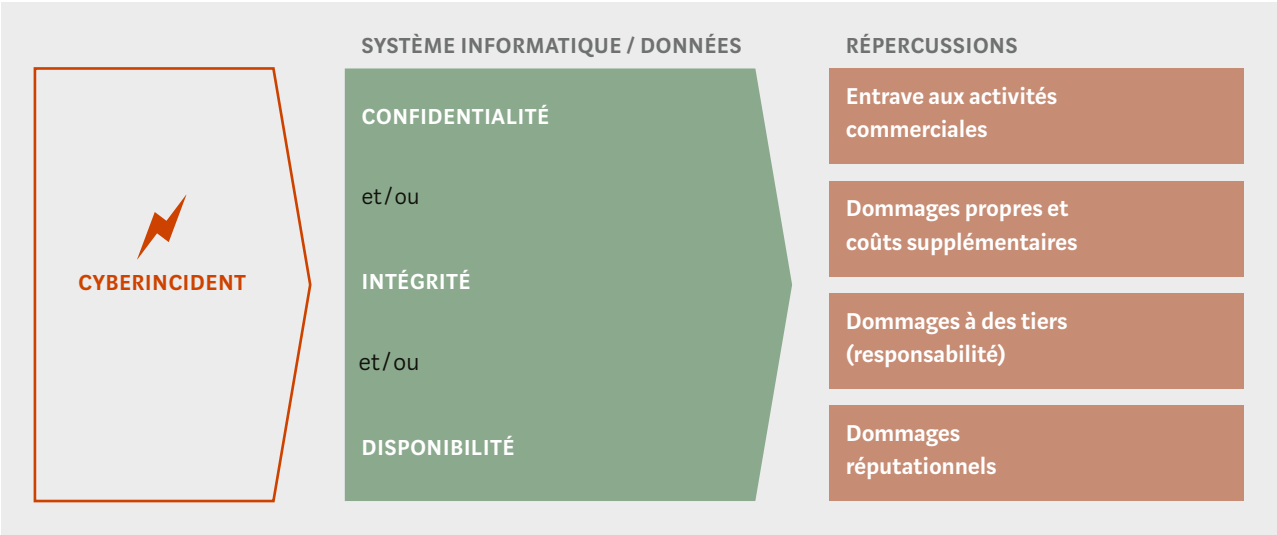
NOTRE APPROCHE GLOBALE DU CYBERRISQUE

La plupart des organisations sont aujourd'hui conscientes que le cyberrisque ne doit pas être confié au seul département informatique, mais qu'il doit être traité dans le cadre d'une approche globale de gestion des risques de l'entreprise (Enterprise Risk Management). Le facteur humain et son comportement d'utilisateur des outils informatiques jouent ici un rôle central. De toute évidence, le cyberrisque représente également un défi managérial et organisationnel. Il requiert en conséquence une combinaison de mesures techniques, administratives, juridiques et financières. Conscients que la sécurité à 100% n'existe pas, nous recommandons d'appliquer des mesures en toute transparence et dans le cadre d'un processus continuellement perfectionné. Chaque organisation devrait s'assurer qu'en cas de cyberincident, le bon fonctionnement de l'entreprise soit garanti et que le retour à la normale soit le plus rapide possible.

REPRÉSENTATION DU CYBERRISQUE

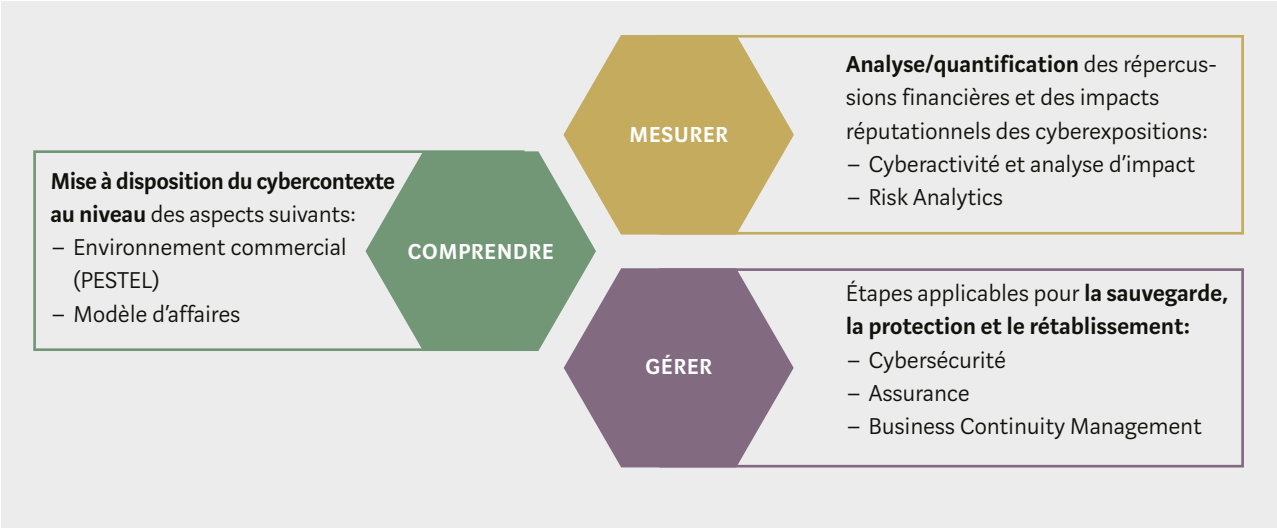
Le risque est une attaque des systèmes informatiques et/ou l'altération des données au niveau de leur confidentialité, de leur intégrité et de leur disponibilité. Les répercussions peuvent être opérationnelles, financières et non-financières, telles qu'une grave perte de confiance des principales parties prenantes.

CYBERRISQUE



APPROCHE

Pour analyser le cyberrisque, nous appliquons une approche sur trois axes.



1

DÉROULEMENT DU PROJET

Avec notre approche «Cyberactivité et analyse d'impact», nous vous aidons à comprendre, mesurer et gérer les cyberrisques. L'atelier interdisciplinaire que nous animons constitue un élément central de la démarche.

COMPRENDRE Analyse de documents et interviews	**MESURER** Atelier interdisciplinaire	**GÉRER** Cyberrapport de projet
– Analyses informatiques – Détermination d'expositions et de vulnérabilités potentielles sur la base de l'analyse de l'environnement et du modèle commercial – Clarification de dépendances ICT – Recensement des infrastructures et des données physiques et numériques	– Développement de cyber-scénarios de menace – Évaluation et priorisation des scénarios selon différents paramètres de coûts (matrice des risques) – Comparaison du benchmark – Élaboration d'un catalogue de mesures d'optimisation du cyberdispositif	– Résumé des conclusions du projet sur la situation des cybermenaces – Présentation de l'utilisation du catalogue de mesures holistiques élaboré et mis à disposition – Informations internes / communication – Sensibilisation

2
CYBERRISQUES

Le terme de cyberrisque est utilisé de manière variée et hétérogène. Il se réfère à divers risques en relation avec la technologie ou les informations d'une entreprise. Du point de vue des assurances, le cyberrisque est défini comme un risque opérationnel qui induit en principe une perte de données, une perturbation ou un dysfonctionnement de systèmes IT/ICT portant atteinte à la confidentialité, la disponibilité ou l'intégrité des informations ou de systèmes d'information.

En Risk Management, le principe de cause à effet est un vieil instrument qui a fait ses preuves. Cet outil permet de mieux comprendre le paysage des cyberrisques d'une entreprise. Celui qui est conscient de ce qui peut être à l'origine des pires scénarios de l'entreprise, peut recourir à une analyse approfondie des causes pour prendre des mesures préventives ciblées, renforçant ainsi la capacité de résilience financière et informatique globale de l'entreprise.

Une perte de données ou une perturbation de systèmes IT/ICT peut avoir des causes aussi bien criminelles que non criminelles (voir p. 10). Selon le code pénal suisse, les causes criminelles sont généralement des actes délictueux en soi, indépendamment du cyberrisque qui en résulte (par ex. acquisition non autorisée de données pour la revente sur le darknet selon l'art. 143 CP ou accès non autorisé dans un système de traitement de données à des fins d'espionnage selon l'art. 143bis CP). D'autres actes délictueux sont par ex. l'infiltration d'un ERP par un malware et donc la manipulation de l'intégrité des données selon l'art. 144bis CP ou le vol d'identité au moyen d'une arnaque au faux président visant à l'enrichissement illégitime selon l'art. 147 CP.

La complexité croissante des systèmes interconnectés offre de nouvelles opportunités aux cybercriminels – qu'il s'agisse de tiers externes, de collaborateurs anciens ou actuels, de concurrents, voire d'organisations étatiques avec différents motifs. Des données sans valeur pour certains peuvent être extrêmement précieuses pour d'autres. Et les entreprises ne sont donc pas protégées contre les cybercriminels simplement parce que la direction pense que leurs propres données ont peu d'utilité pour des tiers. Celui qui cherche à s'introduire dans un système trouvera le moyen de le faire, ce qui génère malheureusement un certain sentiment d'impuissance: il n'y aura jamais de cyberprotection à 100%, et bien moins encore contre une attaque ciblée (Advanced Persistent Threat, APT).

2

CYBERRISQUE: MODÈLE DE CAUSE À EFFET

2.1 RÉPERCUSSIONS FINANCIÈRES

La situation en matière de cyberrisques se complique d'année en année, raison pour laquelle la capacité financière de faire face au risque résiduel doit être prise en compte. Connaître les risques résiduels financiers permet aussi de bénéficier d'une certaine sécurité en vue de leur financement.

Les dommages causés par un cyberincident ne peuvent être ni entièrement ni définitivement quantifiés en raison du manque de données empiriques.

PROPRES DOMMAGES

- Coûts de gestion de crise (informatique judiciaire, conseil juridique, conseil en RP)
- Frais de notification aux parties concernées et aux autorités en cas de perte de données
- Coûts de surveillance des données en cas de perte de données
- Coûts de traitement des demandes de renseignement
- Amendes pour violation de la protection des données
- Coûts de récupération ou de remplacement des données et des systèmes informatiques
- Coûts de maintien en fonctionnement des systèmes informatiques
- Coûts de l'interruption d'exploitation indispensable à la poursuite des activités, y compris perte de bénéfice
- Paiement de rançons et frais consécutifs
- Pertes pécuniaires causées par la fraude en ligne et l'ingénierie sociale et frais consécutifs
- Coûts des dommages causés par des prestataires IT tiers
- Frais pour faire valoir des droits propres violés par des tiers (propriété intellectuelle)
- Frais de défense en lien avec des procédures réglementaires
- Frais de défense en lien avec des risques de responsabilité
- Coûts de prévention ou d'atténuation d'un éventuel risque de responsabilité
- Coûts d'évaluation des dommages
- Coûts consécutifs à un préjudice de réputation

DOMMAGES CAUSÉS À DES TIERS (RISQUES DE RESPONSABILITÉ)

- Paiement de dommages et intérêts à des tiers pour cause de violation de la protection des données ou de la sécurité des données
- Paiement de dommages et intérêts pour atteinte à la personnalité ou à l'honneur
- Paiement de dommages et intérêts pour violation ou perte de la propriété intellectuelle de tiers
- Paiement de dommages et intérêts pour violation du droit de la concurrence, du droit d'auteur, du droit des marques ou de l'obligation de garder le secret
- Paiement de dommages et intérêts ou peine conventionnelle en cas de violation du contrat

2

2.2 RISQUE DE LA CHAÎNE D'APPROVISIONNEMENT IT: QUI LE SUPERVISE?

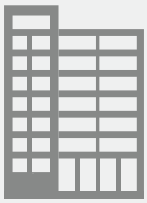
Dans l'économie actuelle interconnectée et fondée sur le numérique, le succès des entreprises dépend largement de l'efficacité de leurs solutions informatiques. Une entreprise qui sous-traite ses services, systèmes, processus ou installations informatiques accroît sa dépendance à l'égard de prestataires tiers. En outre, elle a généralement plus de mal à garder une vue d'ensemble de tous ses fournisseurs et des ressources qui lui font défaut pour surveiller en continu les cyberrisques.

La gestion des partenaires informatiques nécessite aujourd'hui une approche fondée sur le risque, conformément à la demande croissante des investisseurs, des clients sensibilisés ou des autorités de surveillance (par ex. la FINMA ou les instances de surveillance des caisses de pension). Nous vous conseillons d'examiner les fournisseurs IT au regard de vos besoins propres: vos principales parties prenantes et vous obtiendrez/garderez ainsi une vision claire de la chaîne d'approvisionnement IT.

- Quels sont les fournisseurs informatiques dont nous sommes dépendants? Qui traite/transforme quels types de données, dans quel secteur d'activité (données personnelles sensibles, données de production sensibles, conditions contractuelles de clients importants, documents stratégiques, etc.)?
- Quels collaborateurs du fournisseur IT ont accès aux systèmes de notre entreprise et à ses données et combien sont-ils?
- Qui, chez le prestataire, dispose de droits d'administrateur et quels sont ces droits?
- Quelle est la teneur de l'accord de niveau de service (SLA – Service Level Agreement)? Qui assume quelle responsabilité en cas de panne réseau?
- Connaissons-nous les personnes clés et les cyberrisques principaux de la chaîne d'approvisionnement informatique?
- La direction de l'entreprise a-t-elle connaissance des répercussions financières liées à l'action de tel ou tel fournisseur informatique? Quels sont les frais/coûts pris en charge par l'assurance?
- Qui, dans notre entreprise, supervise l'ensemble des points à contrôler avant la signature d'un contrat avec un fournisseur IT?

Graphique ci-contre: Une PME compte en moyenne 20 à 50 prestataires informatiques. Plus le modèle économique de l'entreprise est axé sur l'international et le numérique, plus la chaîne d'approvisionnement IT s'allonge. Il est établi que le facteur humain représente l'un des principaux points faibles de la sécurité informatique et de la cybersécurité. Les trois principaux éléments à connaître sont les suivants: Qui fait partie de notre chaîne d'approvisionnement informatique? Quels sont les membres du personnel de notre entreprise et des prestataires IT qui jouent un rôle clé dans le succès de notre modèle économique? Quelles personnes clés disposent de quelles autorisations et de quels droits d'administrateur? Les réponses à ces questions permettent de définir des mesures préventives ciblées ou de prendre une décision réfléchie concernant la prise en charge du cyberrisque.

ACTEURS DE LA CHAÎNE D'APPROVISIONNEMENT IT DE L'ENTREPRISE



Hébergement de serveurs
- Centre de calcul

Gestionnaire d'infrastructure
- Electricité/eau
- Internet/télécom

Indépendant

Logiciels sur site ou logiciels et hébergement serveur sur site

FinTechs **InsurTechs** **LegalTechs** **MedTechs**

Services de support: fonctions essentielles

Services de support: fonctions auxiliaires

Recherche/ analyses

Conseil juridique et services de consulting

Sous-traitant externe/interne

Surveillance bâtiments

Editeur de logiciels

Start-up d'un autre secteur

Régulateurs/ autorités

Fin de la chaîne d'approvisionnement?

Prestataire cloud (IaaS)
Infrastructure as a Service
- Centre de calcul
- Serveurs physiques
- Systèmes de stockage
- Virtualisation

Prestataire cloud (PaaS)
Platforms as a Service
- Centre de calcul
- Serveurs physiques
- Systèmes de stockage
- Virtualisation
- Système d'exploitation
- Middleware
- Bases de données

Prestataire cloud (SaaS)
Software as a Service
- Centre de calcul
- Serveurs physiques
- Systèmes de stockage
- Virtualisation
- Système d'exploitation
- Middleware
- Bases de données
- Données d'application
- Logiciels standards
- Applications métier

Cloud privé **Cloud hybride**

Multi-cloud **Cloud public**

Cloud com-munautaire **Cloud distribué**

3
GOUVERNANCE D'ENTREPRISE

La cybersécurité est un enjeu de gouvernance. Or, il est difficile de connaître précisément la façon dont les conseils d'administration organisent la surveillance en matière de cybersécurité et dialoguent avec l'encadrement sur ce thème crucial. Chaque sinistre pose la question: le conseil d'administration avait-il ou aurait-il dû avoir connaissance des cyberrisques existants? La réponse peut varier fortement selon les cas, le secteur d'activité concerné ou la modernité des dispositifs de protection des données. Par conséquent, la responsabilité du conseil d'administration sera minutieusement étudiée après chaque gros sinistre cyber. Il est d'autant plus important de prendre des décisions mûrement réfléchies.

3.1 OBLIGATIONS DU CONSEIL D'ADMINISTRATION

En rapport avec le potentiel énorme de dommages résultant des cyberrisques, les conseils d'administration des sociétés anonymes sont soumis à des obligations toujours plus complexes qui sont d'une importance centrale.

OBLIGATIONS TRANSMISSIBLES

Le conseil d'administration est l'organe exécutif d'une société anonyme, pour autant qu'il n'ait pas délégué la direction de l'entreprise. Lors de la délégation de tâches de l'organe exécutif, le conseil d'administration assume la responsabilité des dommages causés par un tiers, s'il ne démontre pas qu'il a pris tous les soins que nécessitaient les circonstances pour choisir ce tiers, le former et le contrôler (art. 716, al. 2, en relation avec l'art. 716b, al. 1, en relation avec l'art. 754, al. 2, CO).

OBLIGATIONS INTRANSMISSIBLES

En ce qui concerne ses obligations intransmissibles et inaliénables, l'ensemble du conseil d'administration en assume obligatoirement l'entière responsabilité. L'intransmissibilité se limite à l'élaboration de décisions, à la prise de décisions ou aux décisions délibérées, par conséquent les tâches de préparation ainsi que l'application de décisions peuvent être confiées à un organe opérationnel.

Selon la doctrine dominante, les obligations suivantes ont valeur d'obligations intransmissibles incombant au conseil d'administration.

- Tâches de surveillance et stratégiques visant à défendre les intérêts de la société ou à préserver ses biens
- Évaluation des risques: dans le cadre du rapport annuel, le conseil d'administration doit, entre autres, réaliser une évaluation des risques commerciaux les plus importants (art. 961c, al. 2, ch. 2, CO). Cela comprend en particulier l'évaluation des risques effectifs du marché, des risques de crédit et de fournitures ainsi que des risques financiers et opérationnels tels que les risques informatiques, les risques liés à la sécurité, aux produits et les risques juridiques, ainsi que les cyberrisques et les perspectives d'avenir pertinentes. Toutes les sociétés qui sont tenues par la loi d'effectuer un contrôle ordinaire doivent établir un rapport de gestion (CO 961 en lien avec l'art. 727).
- Décision relative à la stratégie de financement des risques/stratégie de sécurité IT/ICT.

GOUVERNANCE D'ENTREPRISE – CONDITIONS À LA DÉCISION DE LA DIRECTION

Obligations intransmissibles du conseil d'administration:
- Tâches de surveillance et stratégiques
- Évaluation des plus grands risques
- Décision relative à la stratégie de financement des risques/stratégie de sécurité IT/ICT

La décision de la direction repose sur:
- Des informations appropriées et suffisantes = obtention de toutes les informations juridiques pertinentes en vue des décisions concrètes
- L'examen de tous les avantages et inconvénients des mesures alternatives et de leurs conséquences/ répercussions financières

Les conditions préalables à la décision de la direction sont-elles réunies?

OUI	NON
Décision de la direction = décision délibérée	Décision de la direction ≠ décision délibérée
Business Judgement Rule respectée	Business Judgement Rule non respectée
Aucune violation d'obligation ou aucune responsabilité selon l'art. 754 CO malgré une décision erronée éventuelle	Violation de droit ou responsabilité possible selon l'art. 754 CO

3

3.2 L'IMPORTANCE DE LA DÉCISION DÉLIBÉRÉE

Lors de chaque décision, le conseil d'administration a l'obligation vis-à-vis de l'entreprise de procéder à une préparation, une évaluation et une application diligentes – mais il n'est pas tenu au succès. Il convient donc de mettre en place une procédure de décision diligente et irréprochable. Cela s'applique également à la décision de financement des principaux risques ou à la question de savoir si ces derniers sont transférés ou financés avec des fonds propres.

CONSÉQUENCES D'UNE DÉCISION ERRONÉE DE LA DIRECTION

Dès lors que la décision de la direction repose sur une base d'information appropriée et suffisante et si elle a été élaborée de manière sérieuse, il n'y a pas de violation des obligations légales des organes administratifs. Cela implique que des informations appropriées et suffisantes aient été réunies pour prendre des décisions concrètes et pour peser tous les avantages et inconvénients concernant de possibles alternatives et leurs incidences (cf. ATF 4A_97/2013, consid. 5.2; ATF 139 III 26).

RESPONSABILITÉ DES ORGANES (D&O) – ART. 754 CO

Les experts du secteur de l'assurance font référence aux États-Unis et prévoient qu'en Europe également, les sinistres liés à des cyberattaques feront à l'avenir l'objet d'un nombre de prétentions de plus en plus élevé dans le cadre des assurances D&O et des cyberassurances; cela a des conséquences sur la prise en compte des risques cumulés qui doivent déjà être pris en considération dans le processus de souscription des assureurs et des réassureurs.

Si la direction considère par ex. que les mesures de sécurité sont insuffisantes pour empêcher les piratages informatiques, ou que, de manière indirecte, elles protègent insuffisamment ses actifs, les différents organes peuvent être tenus pour responsables de cette lacune. D'un point de vue juridique, une gestion des cyberrisques absente ou insuffisante ou une décision relative au financement des risques qui n'a pas été prise en connaissance de cause peut, dans certaines circonstances, être qualifiée de violation du devoir de diligence et de fidélité au sens de l'art. 717 CO et éventuellement entraîner une responsabilité en qualité d'organe de la société en vertu de l'art. 754 CO. De même, les obligations omises intentionnellement ou par négligence grave, selon le règlement général de l'UE relatif à la protection des données qui exige la mise en œuvre de certaines normes de sécurité, peuvent renforcer la responsabilité de la direction de l'entreprise.

Outre les membres du conseil d'administration, toutes les autres personnes chargées de la direction de l'entreprise sont soumises à la responsabilité des dirigeants et mandataires sociaux (D&O). À ce titre, les organes informels assument également de manière autonome des tâches de direction et ont une influence décisive sur la formation des décisions au sein de la société.

BUSINESS JUDGMENT RULE (PRINCIPE DE LA LIBERTÉ D'APPRÉCIATION EN AFFAIRES)

La Business Judgment Rule est vérifiée dans le cadre de la responsabilité des organes selon l'art. 754 CO. Selon la formule du tribunal fédéral suisse dans l'arrêt 4A_74/2012, app. 5.1, des tribunaux ont fait preuve de réserve lors du jugement ultérieur de décisions d'entreprises, lorsque ces décisions ont été adoptées selon des processus de décision irréprochables, reposant sur une base d'informations conséquentes et dénués de tout conflit d'intérêt. Un organe de direction ne manque à son devoir que lorsqu'une décision d'entreprise n'est clairement pas défendable. C'est pourquoi les entreprises ont tout intérêt à prendre leurs décisions en toute connaissance de cause et à les documenter de manière exhaustive.

EQUIFAX: LES LIMITES DU PRINCIPE DE LA LIBERTÉ D'APPRÉCIATION EN AFFAIRES

La responsabilité de l'entreprise ou de ses organes de décision peut être mise en cause par des recours collectifs s'il s'avère que la cybersécurité était déficiente lors d'un incident de sécurité des données. Pour déterminer si les décideurs ont respecté leur devoir de diligence, le tribunal va rechercher des preuves afin d'établir s'ils ont agi de manière compétente et intentionnelle et s'ils ont identifié et analysé différentes alternatives avant de prendre une décision réfléchie concernant la gestion des risques existants.

Le récent recours collectif déposé contre Equifax début 2020 montre les limites du principe de la liberté d'appréciation en affaires, ou Business Judgement Rule. Les plaignants reprochent à Equifax d'avoir utilisé le nom d'utilisateur «admin» et le mot de passe «admin» pour sécuriser l'accès à un portail de gestion des litiges en matière de crédit – un tel choix ouvrant la porte aux pirates. Les requérants ajoutent qu'Equifax a laissé la clé de déchiffrement des serveurs contenant les données sensibles sur les mêmes serveurs accessibles au public, de sorte qu'il était facile de supprimer le chiffrement des données. Face à ces affirmations, l'entreprise Equifax aura du mal à prouver qu'elle a assumé ses obligations de diligence à la hauteur du risque. Dans un cas comme celui-là, il est impossible de se réfugier derrière le principe de la liberté d'appréciation en affaires. Pour évaluer si les décideurs ont respecté leur devoir de diligence et enfreint le principe de la liberté d'appréciation en affaires, le tribunal va rechercher des preuves afin d'établir s'ils ont agi de manière intentionnelle et compétente et s'ils ont envisagé et examiné des alternatives aux dernières mesures de sécurité déployées. Les personnes qui ne se préoccupent guère de leur responsabilité en matière de cybersécurité ou qui ont inconsidérément mis l'entreprise en danger ne trouveront aucun secours dans le principe de la liberté d'appréciation en affaires.

LA «STRATÉGIE NATIONALE DE PROTECTION DE LA SUISSE CONTRE LES CYBERRISQUES 2018–2022» SOULIGNE LEUR IMPORTANCE

En Suisse, plusieurs programmes fédéraux dont la «stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022» et le développement de la cyberdéfense au sein de l'armée attestent du caractère essentiel des cyberrisques et du traitement prioritaire dont ils doivent faire l'objet. Les risques cyber et IT sont devenus omniprésents dans le secteur privé comme dans le secteur public, à tel point que personne ne peut en faire abstraction. Plus une entreprise est grande et d'une importance décisive, moins l'on peut se permettre d'ignorer ou de minimiser les mesures de protection nécessaires contre les cyberattaques.

DOCUMENTATION DE DÉCISIONS D'ENTREPRISES

Une décision d'entreprise prise en connaissance de cause doit être consignée dans un procès-verbal (art. 713, al. 3, CO), car des documents tels que des procès-verbaux du conseil d'administration peuvent devoir être produits le cas échéant dans le cadre de procédures d'administration des preuves (art. 160, al. 1, let. b, CPC).

Les avantages, inconvénients et incidences financières des mesures alternatives doivent être documentés en se fondant sur les bases de décision. Les décisions prises en connaissance de cause doivent être dûment justifiées. Les organes de direction de l'entreprise potentiellement impliquées dans des conflits d'intérêt ne devraient pas participer à la prise de décision.

4
PROTECTION ET SÉCURITÉ DES DONNÉES: QUEL RAPPORT AVEC LE CYBERRISQUE?

Les cyberincidents ont quasiment tous pour effet de violer l'intégrité, la disponibilité et la confidentialité des données des personnes et/ou des entreprises. À chaque destruction accidentelle ou illicite de données, à chaque perte, modification ou divulgation de données ou chaque blocage de l'accès aux données (perte d'exploitation), il convient donc d'identifier les lois sur la protection des données et autres lois sectorielles applicables, ainsi que les mesures ou obligations réglementaires qui en découlent. Une violation de la sécurité des données peut résulter d'une cyberattaque criminelle. Mais il se peut aussi que d'autres causes non criminelles, comme par exemple une panne informatique ou un e-mail adressé par erreur au mauvais destinataire, entraînent une perte de données.

Dans le contexte économique et juridique actuel, les dirigeants d'entreprise sont de plus en plus tenus de rendre des comptes et de documenter l'implémentation des mesures réglementaires de protection des données. Est à documenter également la décision réfléchie concernant le mode de mise en œuvre et la priorisation des obligations légales de protection des données. Enfin, il importe de pouvoir justifier la stratégie adoptée en termes de mesures techniques et organisationnelles (MTO).

Les MTO doivent être à la pointe du progrès et conformes aux dernières avancées technologiques. Le caractère «à la pointe du progrès» est une notion juridique indéfinie, dynamique et néanmoins vérifiable par un tribunal. Cette notion recouvre la conformité aux derniers standards de sécurité en vigueur dans le secteur d'activité concerné – des standards susceptibles d'évoluer en permanence. Lors d'un sinistre lié à une cyberattaque, les entreprises affectées doivent apporter la preuve qu'elles ont déployé des mesures techniques et organisationnelles à la pointe du progrès. Les clauses de «conformité aux dernières avancées technologiques» sont courantes dans les contrats de cyberassurance. En l'absence de MTO de pointe, l'assurance peut refuser de couvrir le sinistre ou le couvrir en partie seulement.

LES COÛTS DE VIOLATIONS DE LA LOI SUR LA PROTECTION DES DONNÉES SONT QUANTIFIABLES ET ACTUELLEMENT EN GRANDE PARTIE ASSURABLES:

- Notification aux autorités et personnes concernées
- Coûts des procédures règlementaires
- Amendes pour violation de la protection des données
- Paiement de dommages et intérêts à des tiers pour violation de la protection des données, y compris frais juridiques et de conseil lors de procédures réglementaires, amendes pour violation de la protection des données, coûts de gestion de crise, coûts de notification, etc.

4.1 LA SUISSE ET L'INFLUENCE DE L'UE: QUESTIONS À L'AGENDA D'ICI 2022

Le 25 septembre 2020, le parlement fédéral a adopté la révision de la Loi sur la protection des données (LPD). En raison de la pandémie de COVID-19, la procédure d'élimination des divergences a pris plus de temps que prévu. Jusqu'à l'entrée en vigueur de la loi en 2022, il reste à élaborer les ordonnances correspondantes et à les mettre en consultation. Le parlement a supprimé le délai transitoire initial qui devait accorder deux ans aux entreprises pour s'adapter à leurs obligations. Il est donc d'autant plus important de préparer la mise en conformité à la LPD dès que possible, en faisant appel à des spécialistes qualifiés.

En outre, il reste à savoir si la Commission européenne reconnaîtra l'adéquation de la nouvelle loi. C'est la condition sine qua non pour que les échanges de données entre l'Europe et la Suisse se poursuivent sans entrave. En attendant, c'est la décision rendue par la Commission le 26 juillet 2000 qui continue de s'appliquer car elle ne mentionne pas de date d'expiration. L'Europe n'a pas d'obligation à rendre sa décision concernant l'adéquation de la loi suisse sur la protection des données. Tout dépend de la priorité qu'elle accorde à ce point dans son agenda politique. En tous cas, tant que l'UE n'a pas revu sa décision, la Suisse reste un État tiers doté d'une loi sur la protection des données adéquate aux yeux de l'Europe. Concernant l'agenda politique de l'UE, nous renvoyons à l'arrêt «Schrems II» rendu par la Cour de justice de l'Union européenne le 16 juillet 2020. La CJUE a invalidé avec effet immédiat le bouclier de protection des données dit «Privacy Shield» entre l'UE et les États-Unis, jugeant que le transfert de données personnelles de l'UE vers les États-Unis n'était pas suffisamment sûr au regard de la législation sur la protection des données. Depuis lors, une protection contractuelle additionnelle est donc nécessaire et entraîne un surcoût et une surcharge de travail pour les entreprises.

Les répercussions de l'arrêt Schrems II sont tangibles y compris en Suisse: certes, le bouclier de protection des données Suisse–États-Unis reste valable tant que le Tribunal fédéral ne l'a pas invalidé. Toutefois, le Préposé fédéral à la protection des données et à la transparence (PFPDT) a estimé que ledit bouclier ne garantissait pas non plus la sécurité suffisante pour le transfert de données de la Suisse vers les États-Unis. Cette prise de position est susceptible d'orienter une décision future du Tribunal à propos du bouclier de protection Suisse–États-Unis. Les entreprises suisses qui transmettent des données personnelles vers les États-Unis sont donc tenues de suivre attentivement l'évolution de la situation et de se préparer, le cas échéant, à prendre les mesures adéquates.

4

4.2 OBLIGATIONS DE NOTIFICATION: COMPARAISON SUISSE VS UE

Les entreprises ont intérêt à connaître les différentes catégories de données protégées pour savoir dans quels cas elles sont tenues de déclarer une violation de la sécurité. A titre de mesure préventive et pour minimiser les frais/coûts engendrés par une violation de la protection des données, nous conseillons aux entreprises de se préparer à ce genre d'incident.

	SITUATION JURIDIQUE ACTUELLE CH **Loi féd. sur la protection des données (LPD)** Entrée en vigueur: 01.07.1993 (1er révision 2008)	**SITUATION JURIDIQUE FUTURE CH** **LPD révisée** Entrée en vigueur au plus tôt en 2022 (2e révision)
Catégories de données et obligations de notification correspondantes	– **Données personnelles (personnes physiques et morales)** – **Données personnelles sensibles** Données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales; données sur la santé, la sphère intime ou l'origine raciale ou ethnique; données génétiques; données sur les poursuites ou les sanctions pénales ou administratives; données sur les mesures d'aide sociale.	– **Données personnelles (art. 5, let. a, LPD révisée)** – **Données personnelles sensibles (art. 5, let. c, LPD révisée)** Données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales; données sur la santé, la sphère intime ou l'origine raciale ou ethnique; données génétiques; données biométriques qui identifient un individu de manière unique; données sur les poursuites ou les sanctions pénales ou administratives; données sur les mesures d'aide sociale. – **Protection des données fondée sur le risque: données dont le traitement présente un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.** Le P-LPD s'applique aux risques potentiels pour les personnes concernées, car leur sphère privée dépend dans une large mesure des activités des responsables et sous-traitants. On peut prédire un risque élevé si une entreprise est dans l'obligation de faire une analyse d'impact relative à la protection des données, p.ex. le traitement étendu de données personnelles sensibles ou lorsque des domaines publics sont systématiquement contrôlés à large échelle.
Obligation de notification	**Aucune** obligation de notification légale expresse	**Obligation de notification en cas de violation de la sécurité des données, conduisant très probablement à un risque élevé** pour la personnalité ou les droits fondamentaux de la personne concernée **(art. 24, LPD révisée).** – **Obligation de notification du responsable du traitement:** notification au Préposé fédéral à la protection des données et à la transparence (PFPDT) dans les meilleurs délais. – **Obligation de notification du sous-traitant:** notification au responsable du traitement dans les meilleurs délais. – **Obligation de notification du responsable du traitement:** notification à la personne physique concernée si cela est nécessaire pour sa protection ou si le PFPDT l'exige.
Sanctions en cas d'infraction	**Sanctions pénales:** Amende maximale de CHF **10'000.–**	**Pas d'amende** pour violation de l'obligation de notification. **Responsabilité, demande de dommages-intérêts par la personne concernée et autres sanctions pénales hors RGPD possibles.**

À savoir impérativement:

1. Que s'est-il passé? Quelles sont les catégories de données concernées? 2. Qui doit se charger de la déclaration à l'interne?
3. À qui devons-nous adresser la déclaration? 4. Comment devons-nous déclarer l'incident? 5. Dans quel délai?

SITUATION JURIDIQUE ACTUELLE DANS L'UE/L'EEE

Règlement général de l'UE sur la protection des données (RGPD)

Entrée en vigueur dans l'UE: 25 mai 2018 / dans l'EEE: 20.07.2018

- **Données à caractère personnel**
- **Catégories particulières de données personnelles**
  Données personnelles permettant de connaître l'origine ethnique, les opinions politiques, les convictions religieuses ou idéologiques ou l'appartenance syndicale, ainsi que les informations génétiques, biométriques visant l'identification univoque d'une personne physique, les informations sur la santé ou sur la vie ou l'orientation sexuelle d'une personne physique.

- **Protection des données fondée sur le risque: données dont la perte représente un risque élevé pour les droits et libertés de l'individu**
  Le RGPD ne précise pas dans quels cas il n'existe pas de risque élevé pour les droits et libertés de la personne concernée. Par conséquent, il convient d'évaluer les risques selon l'impact qu'aurait une atteinte à la confidentialité, à l'intégrité et à la disponibilité des données. Par exemple, dans le cas d'une violation de la confidentialité des données personnelles entraînant des préjudices pour la personne concernée: vol de données de connexion ou d'historiques d'achats d'un prestataire, compromission d'informations sur la santé ou de paiement; des e-mails marketing envoyés si bien que n'importe quel destinataire peut également identifier tous les autres destinataires, etc.

Obligation de notification en cas de violation de la protection des données à caractère personnel (art. 33 sq. RGPD)

- **Obligation de notification du responsable du traitement:** notification à l'autorité de contrôle compétente dans les meilleurs délais et au plus tard 72 heures après le constat des faits.
- **Obligation de notification du sous-traitant:** notification au responsable du traitement dans les meilleurs délais.

Notification en cas de «risque élevé» pour les droits et libertés de l'individu concerné

- **Obligation de notification du responsable du traitement:** notification **immédiate** à la personne concernée.

Amendes pour non-respect de l'obligation de notification (art. 83, ch. IV, RGPD)

Amendes administratives jusqu'à 10 millions d'euros ou jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent.

Responsabilité, demande de dommages-intérêts par la personne concernée et autres sanctions pénales hors RGPD possibles.

4

4.3 UN PLAN D'ACTION SUR MESURE VERS LA CONFORMITÉ À LA LPD: LES FONDAMENTAUX

4.4 LISTE DES AMENDES DANS LA LPD RÉVISÉE

Par rapport à la LPD encore en vigueur, la LPD révisée comporte un volet pénal renforcé et prévoit des sanctions plus sévères applicables aux organes responsables qui enfreindraient leurs obligations. Les amendes, dont le montant maximal a été porté à CHF 250 000, visent au premier chef les personnes physiques fautives au sein de l'entreprise (en particulier les décideurs). Exceptionnellement, l'entreprise pourrait être directement sanctionnée par des amdendes pouvant atteindre CHF 50'000. Le Préposé fédéral à la protection des données et à la transparence (PFPT) émet des recommandations, mais n'a pas le pouvoir d'infliger des amendes. Les cantons conservent leur compétence exclusive en matière d'amendes. Seuls les actes intentionnels sont punissables, et non la négligence. Le délai de prescription de l'action pénale est de cinq ans (art. 66 LPD).

SANCTION DES PERSONNES PHYSIQUES PAR DES AMENDES POUVANT ATTEINDRE CHF 250 000.

Art. 60: Violation des obligations d'informer, de renseigner et de collaborer, notamment…
- Violation/omission de l'obligation d'informer la personne concernée en cas de collecte de données personnelles (art. 19)
- Violation/omission de l'obligation d'informer la personne concernée en cas de décision individuelle automatisée (art. 21)
- Violation/omission de l'obligation de renseignement à l'égard de la personne concernée, consistant à lui fournir intentionnellement un renseignement inexact ou incomplet (art. 25-27)
- Infraction à l'obligation de collaborer, consistant à refuser intentionnellement de collaborer avec le PFPDT lors de son enquête ou à lui fournir volontairement des renseignements inexacts (art. 49, ch. III)

Art. 61: Violation du devoir de discrétion, notamment…
- Infraction aux principes relatifs à la communication de données personnelles à l'étranger (art. 16, ch. I, II)
- Infraction aux obligations en matière de traitement des données par des sous-traitants (art. 9, ch. I, II)
- Non-respect des dispositions sur les exigences minimales en matière de sécurité des données (art. 8, ch. III)

Art. 62: Violation du devoir de discrétion dans l'exercice d'une profession, notamment…
- Est punissable quiconque révèle intentionnellement des données personnelles confidentielles portées à sa connaissance dans l'exercice d'une profession qui requiert de telles données.
- Est punissable également quiconque révèle intentionnellement des données personnelles confidentielles portées à sa connaissance dans le cadre des activités qu'il exerce pour le compte d'une personne soumise à l'obligation de garder le secret ou lors de sa formation chez elle.

Art. 63: Insoumission à une décision
- Est passible de sanction quiconque refuse intentionnellement de se conformer à une décision du PFPDT ou d'une autorité de recours.

SANCTION DE L'ENTREPRISE PAR DES AMENDES POUVANT ATTEINDRE CHF 50 000 (ART. 64).

4

4.5 EXCURSUS: LOIS SUR LA PROTECTION DES DONNÉES AUX ÉTATS-UNIS

UNE MOSAÏQUE JURIDIQUE

Aux États-Unis, il n'existe pas de loi générale sur la protection des données comme c'est le cas en Suisse avec la LPD ou dans l'UE avec le RGPD. Les États-Unis disposent de différentes lois valables à l'échelon national, fédéral et régional pour réglementer la protection des données personnelles des individus. En fonction du domaine thématique, ces lois peuvent être complétées ou remplacées par une ou plusieurs des plus de 20 lois sectorielles sur la protection des données, valables par exemple dans le domaine de la finance, de la santé ou du commerce. Il convient de vérifier au cas par cas la façon dont ces différentes lois entrent en concurrence.

Contrairement à la Suisse et à l'UE, les États-Unis ne considèrent pas la protection des données comme un droit fondamental mais l'intègrent au droit de la consommation. Aux États-Unis, la surveillance légale de la protection des données incombe par conséquent à la Federal Trade Commission, l'agence également chargée de la protection des consommateurs et de la concurrence. Il n'existe pas aux USA d'autorité indépendante chargée de la protection des données comme en Suisse ou dans l'UE.

NOTIFICATION DE VIOLATION DE DONNÉES

Les 50 États américains ont tous adopté des lois obligeant à déclarer les violations de données aux autorités, ou Data Breach Notification Laws. En cas de perte de données ou de divulgation accidentelle de données, l'entreprise en cause est tenue d'en informer le gouvernement de l'État concerné.

LA CALIFORNIE EST UN PIONNIER EN MATIÈRE DE LOIS SUR LA PROTECTION DES DONNÉES

En 2002, la Californie fut le premier des 50 États fédérés à promulguer une loi concernant la déclaration des violations de sécurité des données (§ 1798.82 California Civil Code). Depuis l'adoption du California Consumer Privacy Act de 2018 (CCPA, en vigueur depuis le 1er janvier 2020), elle fait figure de modèle sur le plan du droit de la protection des données. Le CCPA s'applique sur le territoire de la Californie et confère aux consommateurs le droit d'accéder à leurs données personnelles détenues par des entreprises et de supprimer ces données. En outre, cette loi oblige les entreprises à garantir aux consommateurs une sécurité adéquate de leurs données. Du fait de sa portée extraterritoriale, le CCPA peut s'appliquer y compris à des entreprises qui ne sont pas physiquement implantées en Californie.

1. Conditions d'application du CCPA

- Collecter des informations personnelles de résidents californiens; et
- exercer une activité lucrative en Californie; et
- répondre à un ou plusieurs des critères suivants: réaliser un chiffre d'affaires annuel de plus de 25 millions de dollars; traiter les données personnelles d'au moins 50 000 consommateurs ou appareils; tirer au moins 50% de ses recettes annuelles de la vente d'informations personnelles de consommateurs.

2. Risques pour les entreprises

Amendes d'un montant de $ 2 500 à $ 7 500; actions collectives au civil et versement de dommages-intérêts à hauteur soit de $ 100 à $ 750 par consommateur concerné et par incident, soit des dommages réels subis, selon le montant s'avérant le plus élevé; procédure juridique y compris pour les entreprises étrangères dans la mesure où le CCPA le prévoit.

3. Efficacité du CCPA

L'efficacité de la loi fait débat, notamment parce que le texte ne prévoit pas de mesures de sécurité obligatoires ni de sanctions pour non-respect et fixe des amendes relativement faibles par rapport au RGPD en particulier.

5
ASSURABILITÉ DES CYBERRISQUES

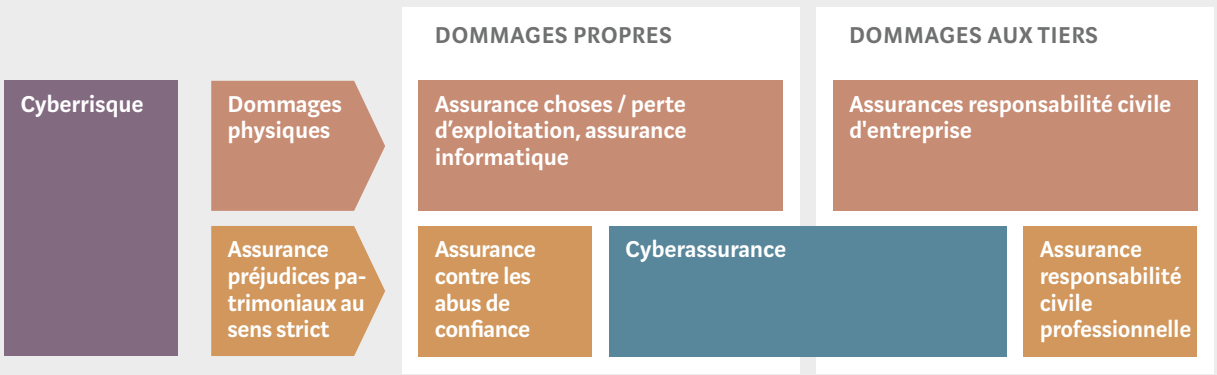
L'assurance de cyberrisques met le secteur des assurances devant de nouveaux défis. Les risques tels que l'incendie, le matériel et l'interruption d'exploitation bénéficient d'une répartition naturelle du risque. Il est peu probable que des centaines de grands incendies surviennent en Suisse le même jour. En revanche, un cyberrisque peut se propager de manière virale et nuire simultanément à de nombreuses entreprises. Pour les assureurs, il peut en résulter un risque de cumul difficilement calculable, dès lors qu'un même sinistre peut concerner plusieurs risques assurés auprès d'un même assureur.

L'industrie de l'assurance a donc mis au point des polices spéciales afin de couvrir les principaux aspects du cyberrisque encouru par les entreprises. Les assureurs développent une connaissance très pointue du cyberrisque puisqu'ils le couvrent au moyen d'une solution d'assurance à part, dotée de son propre processus de souscription. Quant aux clients, ils bénéficient d'une solution d'assurance complète dédiée au cyberrisque.

En outre, afin de mieux contrôler le risque de cumul, les assureurs n'incluent plus désormais qu'une garantie limitée contre les risques, voire aucune garantie, dans leurs polices d'assurance conventionnelles. Malgré ces changements, l'étendue de la couverture n'apparaît pas de manière transparente dans toutes les polices. Il existe toujours des contrats offrant une couverture dite «silencieuse» du risque cyber (silent cyber cover). C'est pourquoi il est crucial, mais aussi complexe, de coordonner polices traditionnelles et polices spéciales pour éviter autant que possible les lacunes de couverture. Pour nos clients, nos experts en cyberassurance réalisent une analyse complète des lacunes dans chaque cas.

Le graphique ci-après présente une imbrication possible de la cyberassurance parmi les polices conventionnelles. Une cyberassurance type couvre les préjudices patrimoniaux au sens strict et englobe les dommages propres et les dommages aux tiers.

LE CYBERRISQUE VU PAR L'INDUSTRIE DE L'ASSURANCE



5

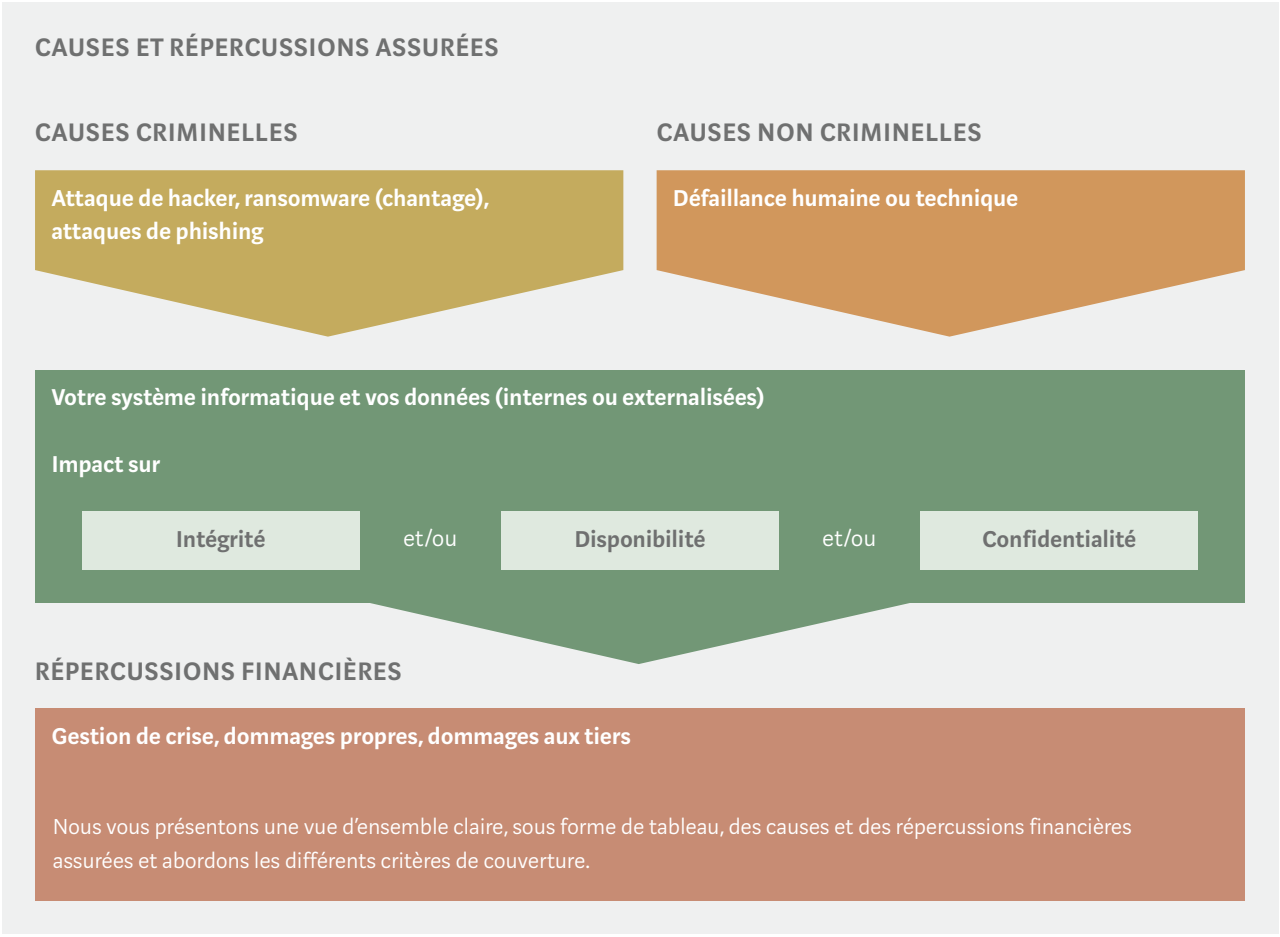
5.1 CYBERASSURANCE: DOMMAGES ASSURABLES

Un même module de couverture n'englobera pas toujours les mêmes garanties d'un assureur à un autre. À partir de l'analyse du cyberrisque auquel votre entreprise est exposée, nous évaluons pour vous les différentes offres des assureurs.

Le schéma ci-contre présente l'étendue de la couverture.

- La gestion de crise englobe les prestations de services que l'assureur met à votre disposition par le biais de partenariats externes dans le domaine de l'informatique judiciaire, du conseil juridique et du conseil en RP.
- Le domaine de l'assurance comprend les dommages propres (perte d'exploitation et frais/coûts supplémentaires) et les dommages aux tiers. Les dommages propres désignent les frais/coûts occasionnés par un cyberincident. Les dommages aux tiers correspondent à la prise en charge des demandes légitimes de dommages-intérêts et à la défense en cas de demandes illégitimes.

Les négociations menées par Kessler déterminent l'étendue de la couverture proposée par les prestataires pour les causes et pour les répercussions financières présentées dans le graphique. Il en va de même pour l'étendue de la couverture dans le domaine de l'externalisation informatique.


CAUSES ET RÉPERCUSSIONS ASSURÉES
CAUSES CRIMINELLES
CAUSES NON CRIMINELLES
Attaque de hacker, ransomware (chantage), attaques de phishing
Défaillance humaine ou technique
Votre système informatique et vos données (internes ou externalisées)
Impact sur
Intégrité
et/ou
Disponibilité
et/ou
Confidentialité
RÉPERCUSSIONS FINANCIÈRES
Gestion de crise, dommages propres, dommages aux tiers
Nous vous présentons une vue d'ensemble claire, sous forme de tableau, des causes et des répercussions financières assurées et abordons les différents critères de couverture.

5

5.2 ASSURANCE CONTRE LES ABUS DE CONFIANCE

Pour le secteur de l'assurance, les préjudices patrimoniaux au sens strict résultant d'une attaque par ingénierie sociale ne constituent pas à proprement parler des cyberrisques car les criminels opèrent sans intrusion dans le système informatique. Une assurance contre les abus de confiance peut couvrir ce risque.

Bien que la cyberassurance reconnaisse n'importe quelle attaque de hacker comme une cause assurée, elle ne couvre pas toutes les répercussions financières qui en découlent. Les délits basés sur la technique de l'ingénierie sociale sont un exemple connu. Dans le cas d'une attaque de phishing, les coûts de récupération des données après propagation d'un virus sont couverts par une cyberassurance. En revanche, le préjudice patrimonial direct que constitue un transfert bancaire par usurpation d'identité n'est pas ou peu couvert. Il existe deux raisons à cela.

D'une part, ces attaques se déroulent généralement sans intrusion dans le système informatique et utilisent simplement des e-mails provenant d'expéditeurs dont l'adresse a été falsifiée. Dans ce genre d'e-mail, il sera question d'un changement de coordonnées bancaires ou d'une prétendue notification de la banque, avec un lien sur lequel on vous invite à cliquer pour mettre à jour vos données de connexion. Parfois, les pirates peuvent aussi vous contacter par téléphone en se faisant passer pour un client, le support informatique ou le PDG. D'autre part, le marché de l'assurance considère que l'assurance contre les abus de confiance offre déjà une solution pour protéger les comptes de l'entreprise contre les infractions basées sur l'outil informatique et garantir le préjudice strictement patrimonial.

Il est donc intéressant de vérifier précisément si le besoin en assurance implique de contracter en plus une assurance contre les abus de confiance. En effet, le télétravail et les modifications qu'il entraîne au niveau des processus organisationnels et des autorisations d'accès aux systèmes informatiques de l'entreprise favorisent grandement les infractions criminelles basées sur l'informatique. Mais toutes les polices n'assurent pas ce type de préjudice. Elles couvrent principalement le risque d'enrichissement personnel illicite d'un collaborateur.

5.3 ASSURANCE CHOSES ET PERTE D'EXPLOITATION, ASSURANCE TECHNIQUE

Face à l'augmentation des sinistres de type cyber, les assureurs de choses ont réagi et adapté ou précisé leurs conditions. Les polices actuelles ne comportent plus de couverture silencieuse du risque cyber. Autrement dit, elles ne laissent plus de doute sur ce qui est couvert ou non. La couverture d'assurance pour les sinistres choses de type cyber est explicitement décrite dans les polices. La mise en œuvre peut toutefois varier fortement d'un assureur à un autre.

En règle générale, il doit exister un sinistre choses physique, qui occasionne ensuite une perte d'exploitation. Les données elles-mêmes ne sont pas des choses et ne peuvent donc pas être l'objet d'un sinistre au sens de cette assurance. En revanche, si le support sur lequel se trouvent les données est endommagé ou détruit, par exemple lors d'un incendie, l'assurance couvre alors les coûts de récupération des données à partir d'une sauvegarde. Mais l'entreprise n'est pas indemnisée pour les données elles-mêmes.

Une cyberattaque ciblée peut par exemple déclencher un incendie, qui détruit un équipement informatique, une machine de production ou un bâtiment. Cette destruction peut ensuite causer une perte d'exploitation dans le pire des scénarios. L'assurance choses et perte d'exploitation couvre alors le sinistre puisqu'il existe bien des dommages physiques causés par le feu.

Le principe est le même en cas de défaillance d'un fournisseur important. Cela peut être par exemple un fournisseur d'énergie ou un prestataire informatique. Il doit s'être produit un sinistre choses, couvert par votre propre police d'assurance au titre des dommages de répercussion. Autrement dit, l'interruption de fourniture de courant ou la panne chez le prestataire informatique doivent résulter par exemple d'un incendie. Une coupure de courant ou une indisponibilité des données liée à un cyberincident qui a par exemple verrouillé l'accès aux données ne constitue pas un sinistre choses.

Les assurances techniques, quant à elles, englobent les assurances d'équipements électroniques et de machines. Le spectre des événements couverts par ces assurances est en général un peu plus large du fait de l'approche tous risques. Mais, ici encore, l'existence d'un sinistre choses physique est une condition requise. En conséquence, le simple arrêt d'un équipement informatique ou d'une machine à la suite d'un cyberincident n'est pas couvert par l'assurance.

6
DU CYBERINCIDENT AU SINISTRE COUVERT PAR LA CYBERASSURANCE

Une cyberassurance sur quatre est amenée à traiter des sinistres. De ce fait, les entreprises affectées et les experts gagnent en compétences. Les assureurs ont progressé continuellement dans le domaine de la gestion de crise et du règlement des sinistres et peuvent désormais démontrer l'efficacité des mesures préventives aux preneurs d'assurance. Kessler vous accompagne tout au long du processus pour optimiser le règlement de chaque sinistre.

	CYBERINCIDENT	SINISTRE COUVERT PAR LA CYBERASSURANCE
AVANT L'INCIDENT	**Mettre au point le processus de gestion des cyberrisques** – Identifier, protéger, détecter, réagir et assurer une surveillance continue – Vérifier les clauses relatives à la responsabilité dans les contrats avec les clients, les fournisseurs et les prestataires IT – Vérifier les interdépendances des fournisseurs et des prestataires IT – Mettre en œuvre des mesures préventives, par ex. des formations de sensibilisation du personnel – Prendre une décision réfléchie concernant le financement propre ou externe en matière de cyberincidents **Élaborer un plan de réponse aux incidents, un plan de continuité d'activité et un plan de reprise après sinistre** – Sélectionner des experts en informatique judiciaire, conseil juridique et conseil en RP – Simuler une situation dans laquelle les systèmes informatiques sont indisponibles ou non fiables durant quelques jours ou semaines et mettre en place des canaux de communication de substitution – Tester régulièrement les plans et analyser les résultats	**Mesures préparatoires** – Sélectionner des experts en informatique judiciaire, conseil juridique et conseil en RP, établir des contrats avec eux et conduire des réunions d'intégration **Connaître sa police d'assurance** – Communiquer le numéro d'urgence aux personnes impliquées – S'acquitter des obligations contractuelles (par ex. devoir de notification en cas d'aggravation du risque)

	CYBERINCIDENT	SINISTRE COUVERT PAR LA CYBERASSURANCE
PENDANT	**Survenance du cyberrisque** – Perte de données – Dysfonctionnement informatique/TIC – Cybercriminalité/crime en ligne **Mesures immédiates** – Consulter le plan de réponse aux incidents – Consulter les experts sélectionnés en informatique judiciaire, conseil juridique et conseil en RP – Déclencher et coordonner les mesures définies (voir aussi Notifications) – Documenter continuellement le cyberincident en termes de déroulement et de frais/coûts **Notifications** – Vérifier les obligations de notification légales ou effectuer une déclaration volontaire auprès des autorités et des parties concernées – Faire intervenir la police à des fins de conservation des preuves – Informer le personnel, les médias et/ou vérifier l'obligation de publicité ad hoc	**Mesures immédiates** – Composer le numéro d'urgence: la consultation des experts en informatique judiciaire, conseil juridique et conseil en RP est en cours – Signaler immédiatement le cyberincident à Kessler et/ou à l'assureur et poursuivre le travail en étroite collaboration **Autres mesures** – Faire approuver préalablement toutes les dépenses par l'assureur – Respecter l'obligation de réduire le sinistre – Désigner et impliquer un expert dès que possible pour quantifier le sinistre – Traitement du dossier avec l'assureur: remettre les documents pour l'appréciation des faits et l'examen de la couverture; obtenir un acompte éventuel
APRÈS	**Enseignements tirés** – Valider la prestation des experts en informatique judiciaire, conseil juridique et conseil en RP impliqués – Réviser le plan de réponse aux incidents, le plan de continuité d'activité et le plan de reprise après sinistre	**Enseignements tirés** – Valider la prestation du ou des assureurs et des experts en informatique judiciaire, conseil juridique et conseil en RP impliqués – Réviser la somme d'assurance et la franchise choisies

7
LE PROCESSUS EN DEUX PHASES

Notre équipe, spécialisée en gestion de cyberrisques et en cyberassurance, vous conseille sur le choix de votre solution personnalisée de cyberassurance. Elle dispose de vastes connaissances spécialisées et de l'expérience correspondante. Dans l'intérêt de nos clients, nous sommes en contact étroit avec Marsh, notre partenaire réseau qui développe à l'échelle mondiale des solutions de cyberassurance. Nous vous conseillons un processus en deux phases pour vos besoins en cyberassurance. Cela étant, il est également possible de commencer directement par la phase 2.

7.1 PREMIÈRE PHASE: DIALOGUE SUR LES CYBERRISQUES

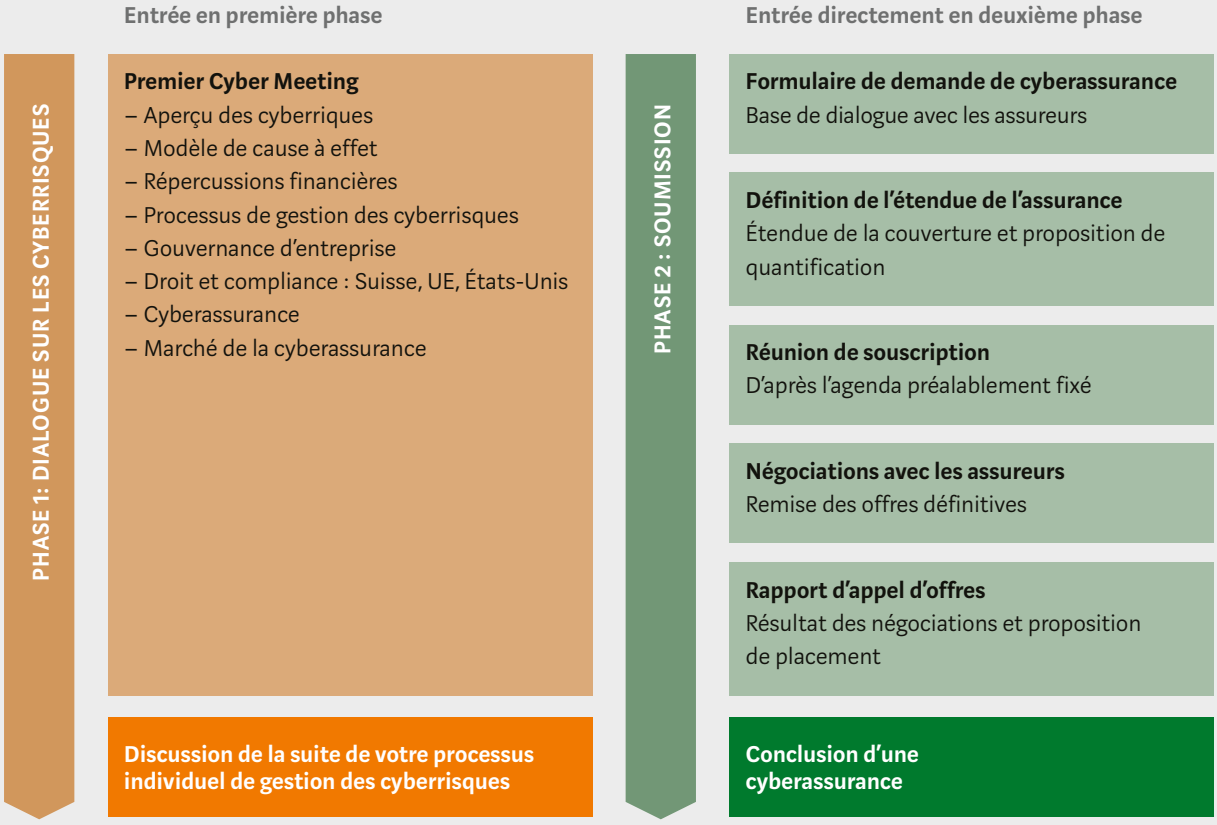
Dans le cadre de la gestion des risques et pour soutenir une gouvernance d'entreprise optimale, nous analysons avec vous les cyberrisques spécifiques à votre entreprise et à votre branche, les processus d'information et d'organisation internes qui y sont liés ainsi que les aspects juridiques en constante évolution, surtout en Suisse, dans l'UE et aux États-Unis. Cela nous sert de base pour la planification des prochaines étapes.

7.2 DEUXIÈME PHASE: DEMANDE D'OFFRES FERMES

Nous recommandons d'engager des négociations avec trois prestataires de premier plan. Lorsque vous recevez le formulaire de demande de cyberassurance, nous définissons ensemble l'étendue de l'assurance et débutons l'appel d'offres. Avant de soumettre leur offre, les assureurs choisis ont besoin d'informations spécifiques concernant votre entreprise, sa structure et son environnement économique, son organisation informatique, la maturité de la sécurité de vos systèmes IT et la gestion du risque. Il convient généralement de leur fournir ces informations de manière orale, lors d'une présentation ou d'une conférence téléphonique. Puis des négociations ont lieu avec chacun des assureurs.

Ces derniers élaborent ensuite des offres fermes. Kessler en synthétise les résultats dans son rapport d'appel d'offres et les commente directement avec vous. Sur cette base, vous pouvez décider de souscrire une cyberassurance. À travers l'analyse coûts-bénéfices d'une cyberassurance, vous prenez une décision sur le mode de financement des risques. À notre avis, vous vous conformez ainsi aux exigences de la gouvernance d'entreprise (principe de la liberté d'appréciation en affaires), qui supposent d'intégrer le cyberrisque en connaissance de cause dans le processus de gestion des risques de l'entreprise.

LE PROCESSUS EN DEUX PHASES
ARRIVER À UNE DÉCISION EN TOUTE CONNAISSANCE DE CAUSE GRÂCE À UN DIALOGUE APPROFONDI SUR LES RISQUES



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 1 000 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 300 collaborateurs travaillant au siège à Zurich et sur les sites de Bâle, Berne, Genève, Lausanne, Lucerne, Neuchâtel, Saint-Gall 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 active dans plus de 130 pays et le principal courtier en assurances et conseiller en gestion des risques et fait partie de Marsh & McLennan (NYSE : MMC).

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

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

Marsh Network