ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni
Swiss Insurance Association

Document de principe

Bureau responsable	Comité Réassurance
Organe	Groupe de travail consacré aux cyberrisques
Date	22 février 2018
Thème	**Document de principe de l'ASA sur les cyberrisques**

Résumé

Rien qu'en Suisse, la facture annuelle des cyberrisques s'élève approximativement à 9,5 milliards de francs, et la tendance va croissant. Dans le contexte de la révision de la stratégie nationale de protection de la Suisse contre les cyberrisques, le présent document de principe décrit le rôle des assurances en matière de renforcement de la gestion des cyberrisques. Il énumère également les conditions requises pour l'assurabilité des cyberrisques et aborde le rôle de l'Etat et des politiques au regard de la constitution d'un marché de l'assurance pérenne dédié aux cyberrisques.

Les assureurs secondent les entreprises en matière de gestion des risques et, ce faisant, assument toute une série de missions importantes pour le bon fonctionnement de l'économie. Or, les cyberrisques ne sont pas sans risque, justement, pour les assureurs :

- accumulation,
- manque de données,
- asymétrie de l'information,
- obligations d'assurance.

L'interconnectivité croissante de l'économie ainsi que les monocultures de matériel et de logiciels informatiques accroissent le risque qu'un cyberincident touche plusieurs entreprises en même temps et provoque alors des dommages considérables au niveau macroéconomique. Nous avons étudié cinq scénarii d'accumulation et évalué leur potentiel de dommages pour l'économie dans son ensemble et le secteur de l'assurance en particulier. Ces dommages potentiels s'élèvent à quelque 12 milliards de CHF dans le cas extrême du scénario « Réseau électrique » (environ 2 pour cent du produit intérieur brut de la Suisse, PIB) et peuvent atteindre 2,5 milliards de CHF pour les autres scénarii (soit 0,4 pour cent du PIB au maximum).

Du fait de la pénétration encore très faible sur le marché de cyberassurances spécifiques et au regard des capacités qui y sont déjà mises à disposition par les assureurs et les réassureurs, l'industrie de

l’assurance est actuellement en mesure d’assumer des cybersinistres majeurs. Toutefois, si la pénétration du marché continue sur sa lancée, il faudra étudier de plus près la capacité de résistance de l’industrie de l’assurance à de tels dommages.

En cas de cyberattaques d’infrastructures d'importance critique et de dommages en découlant provoqués aux valeurs matérielles et potentiellement aux personnes, l’industrie de l’assurance ne propose pas de couvertures globales pour les cas extrêmes, car de tels événements majeurs risqueraient rapidement d’excéder les capacités du secteur de l’assurance. Des solutions possibles doivent être examinées plus avant comme dans le cas des couvertures contre les attentats terroristes ou dans celui du pool des dommages naturels offrant un financement public à partir d’un certain seuil. Le peu de données disponibles complique la tâche des assureurs qui ont du mal à proposer des produits adéquats à des prix reposant sur les risques effectifs. Instaurer une obligation générale de signaler tout cyberincident pourrait s’avérer utile, surtout si cette obligation ne porte pas uniquement sur les atteintes à la protection des données mais comprend également d’autres types de cyberincidents. L’expérience montre néanmoins que, dans certaines circonstances, un signalement spontané de tels incidents est préférable à une obligation légale, car la cellule chargée du signalement récolte alors généralement des données de meilleure qualité. Par contre, dans un tel cas, les données obtenues ne sont pas forcément représentatives de l’ensemble des acteurs économiques. La discussion est donc ouverte sur la question de savoir si, concernant les cyberincidents, un signalement spontané permettrait effectivement de récolter des données de meilleure qualité qu'une obligation de signalement.

En la matière, l’échange de données joue aussi un rôle non négligeable. L’échange de données doit se dérouler dans un cadre soumis au droit de la concurrence. Par ailleurs, le secteur de l’assurance peut tout à fait s’organiser seul avec les autres acteurs du marché.

Les asymétries d'informations entre le preneur d’assurance et l’assureur sont susceptibles d’encourager l’antisélection ou de contribuer au fait que le preneur d’assurance tire profit de l’assurance au delà du but premier de celle-ci (« aléa moral »). Ces deux phénomènes sont des facteurs qui restreignent fortement l’assurabilité des risques. L’une des asymétries possibles de l’information dans le domaine des cyberrisques peut être contrée par l’instauration de normes minimales en matière de cybersécurité.

De telles normes minimales devraient reposer sur des principes et ne devraient pas surcharger ni solliciter outre mesure les entreprises censées les appliquer.

Il faut alors étudier avec précision la meilleure manière d’introduire et de mettre en œuvre de telles normes :

- Normes minimales prescrites par la loi
- Obligation légale d’élaborer des normes minimales sectorielles

– Normes minimales sectorielles non prescrites par la loi et néanmoins obligatoires, par exemple, pour obtenir la couverture d'assurance ou participer à certaines chaînes de distribution.

Un point important qui va au delà de l'introduction de normes minimales consiste dans la prise de conscience par les entreprises des cyberrisques qu'elles encourent. Cette prise de conscience peut être facilitée, par exemple, par des campagnes de sensibilisation et le travail dans le cadre de partenariats public-privé incluant également l'industrie de l'assurance.

Les assurances obligatoires touchent essentiellement les domaines où une activité ou un ouvrage peuvent entraîner des dommages à des tiers (par ex. pour les catégories comme les médecins, les détenteurs de véhicule, les centrales nucléaires, les barrages). Les autres assurances obligatoires, surtout celles couvrant les risques liés aux forces de la nature, portent sur les dommages propres subis pas les assurés. Une telle obligation oblige les acteurs du marché à transférer leur risque financier (en tant que lésés ou responsables potentiels) sur un tiers (l'assureur) et présuppose que le risque soit intégralement assurable. Or, ce critère de l'assurabilité n'est que partiellement rempli en matière de cyberrisques. Par ailleurs, les entreprises pourraient être incitées à réduire leurs investissements dans la cybersécurité puisqu'elles seraient de toute façon assurées. En conséquence, une telle mesure irait à l'encontre du souhait d'un renforcement de la cybersécurité en général.

L'Association Suisse d'Assurances ASA estime que le Conseil fédéral devrait appliquer les huit mesures suivantes, de préférence de concert avec les acteurs économiques.

1 Déclencher une plus grande prise de conscience des petites et moyennes entreprises (PME) concernant les cyberrisques qu'elles encourent. Il faut mener ou soutenir des campagnes de sensibilisation en ce sens. D'une manière générale, il faut veiller à sensibiliser l'opinion publique aux cyberrisques (prise de conscience, *awareness*). A cet effet, il est nécessaire d'élaborer et de mettre en œuvre un concept de communication approprié.

2 Il faut encourager le développement de compétences et l'élargissement des connaissances. Il s'agit notamment d'accroître les capacités d'évaluation et de représentation de la situation en termes de cybermenaces.

3 Il faut introduire ou optimiser la gestion de la résilience au niveau de l'entreprise, en particulier dans un souci de prévenir le risque économique d'accumulation et, par voie de conséquence, de préserver l'assurabilité future des cyberrisques.

4 L'élaboration et l'introduction d'une norme minimale sont indispensables et rencontrent une large adhésion. Il convient donc d'élaborer une (norme fédérale) et/ou plusieurs normes (normes sectorielles) et d'œuvrer à leur introduction.

5 L'introduction d'un signalement obligatoire des cyberincidents est plutôt bien accueillie par l'ensemble des parties prenantes. En conséquence, les autorités fédérales compétentes peuvent d'ores et déjà examiner la forme que doit prendre une telle obligation de signalement et statuer sur son introduction.

6 La Confédération doit mettre en place un ensemble de services à l'intention des différents types d'entreprises existants (par ex. conseils, renseignements, etc.).

7 Afin de réduire le nombre de sinistres à venir, les cybercriminels doivent pouvoir faire l'objet de poursuites pénales systématiques, ceci tant au niveau national qu'international.

8 Une coopération s'impose à l'échelle nationale comme internationale (par ex. statistique commune sur les dommages, gestion de crise bien organisée, identification des menaces, etc.), également dans le secteur de l'assurance.

En complément aux mesures précitées pour lesquelles l'Etat doit assumer un rôle prépondérant, l'industrie de l'assurance se dispose à examiner les initiatives suivantes :

9 Outre les cyberrisques qui menacent le secteur privé, il convient également d'analyser ceux mettant en péril les institutions et les services publics afin de pouvoir apporter un soutien optimal en matière de gestion des cyberrisques aussi à ces niveaux.

10 Il faut étudier et coordonner avec les pays voisins la conception de conditions modèles relatives aux cyberassurances.

11 L'industrie de l'assurance doit promouvoir le rassemblement de connaissances dans le domaine du cyberconseil et du règlement des dommages.