ASA | SVV

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

# DISCOURS

de Severin Moser, membre du comité directeur de l'ASA
Evénement **Conférence de presse annuelle de l'ASA**
Date 18 janvier 2018
Lieu Zurich

**Les cyberrisques – Le point de vue des assureurs**

*Seul le texte prononcé fait foi.*

Mesdames et Messieurs,

Le monde est de plus en plus interconnecté … Avec l'Internet des objets, 50 milliards d'appareils seront interconnectés d'ici 2020. Du réfrigérateur à la puce électronique incorporée dans le corps humain en passant par la radio et la télévision. Quelque 250 millions de véhicules sillonneront les routes, enregistreront et traiteront des données en permanence, les ajusteront avec les satellites et d'innombrables applications – voire circuleront pour certains en toute autonomie.

Autant d'opportunités immenses à saisir. Or, là où il y a des opportunités, il y a aussi des risques. Cyberattaques, vols et abus de données ainsi que défaillances des systèmes sont seulement quelques exemples des menaces réelles de la numérisation. Les coûts annuels moyens des cyberdommages sont estimés à 450 milliards de dollars américains au niveau mondial. C'est plus de deux fois le coût des catastrophes naturelles qui se monte en moyenne pluriannuelle à près de 200 milliards de dollars d'après Swiss Re. Il ressort d'une étude McAfee que les coûts annuels des cyberdommages ont atteint jusqu'à 9,5 milliards de francs suisses rien qu'en Suisse.

**Savoir identifier les risques graves**

Ce sont des coûts énormes. Et des risques énormes. Les hommes veulent se protéger contre les risques. Or se protéger présuppose avoir conscience des risques. Il semble que dans notre pays, il n'y ait pas encore de véritable prise de conscience des risques liés à la numérisation et plus particulièrement des cyberrisques. Les PME surtout sont très en retard. Tel est le constat du sondage réalisé par l'institut gfs sur mandat notamment de l'ASA et portant sur les « Cyberrisques dans les PME suisses ».

D’après cette étude, 56 pour cent des dirigeants d’entreprise interrogés pensent être bien à très bien protégés contre les cyberattaques. Le risque d’être victime d’une attaque informatique est estimé comme faible par les entreprises : seules 10 pour cent considèrent que le risque de se voir exposées à une interruption d’activité d’une journée entière est élevé. Et seulement 4 pour cent des PME estiment élevé à très élevé le risque de voir leur existence menacée. Ces chiffres illustrent clairement à quel point la prise de conscience des risques est encore très faible sur ce segment au niveau des décisionnaires – mais pas au niveau des informaticiens.

Toute solution spécifique présuppose toujours une analyse ciblée des risques. D’après le baromètre des risques 2018 d’Allianz établi à partir d’un sondage réalisé auprès de 2 000 experts de par le monde, une interruption d’activité demeure le risque d’entreprise le plus important au niveau mondial. En Suisse aussi, ce risque est toujours à la première place des préoccupations, car une interruption d’activité peut avoir des conséquences gravissimes pour l’existence même d’une entreprise.

Entraînent potentiellement une telle interruption les cyberattaques comme les vols de données, les piratages informatiques ou les rançongiciels (ransomware). Les cyberrisques progressent partout dans le monde. En Suisse, ils sont en troisième position du classement des risques en 2018.

**Cyberassurances – Evolution du marché**

Le marché des cyberassurances est encore petit, mais il progresse. Les experts de Swiss Re estiment actuellement les recettes annuelles de primes pour les cyberassurances à 400 millions de dollars américains déjà pour le seul marché européen. A titre de comparaison : les recettes de primes découlant des assurances automobiles sont estimées à 161 milliards de dollars en Europe. D’après une récente étude de KPMG, le volume des cyberprimes en Suisse devrait atteindre près de 2,2 milliards d’euros d’ici 2036. Trois quarts de ce volume découleraient des petites entreprises et des particuliers.

Le calcul de la prime demeure encore un véritable casse-tête, car les risques sont difficiles à évaluer puisqu’il n’existe pas de données de base qui permettraient un calcul modélisé. Sans parler de la fulgurance du progrès technologique qui apporte sans cesse son lot de nouveaux cyberrisques et rend les cyberproduits de plus en plus complexes. Tout cela montre bien que la cybersécurité va bien au-delà de la simple couverture d’assurance. La protection s’accompagne d’un besoin accru en conseil et en services permettant d’expliquer et d’identifier les attaques possibles.

Outre Allianz, d’autres membres de l’ASA comme Zurich, la Mobilière ou encore Generali, pour n’en citer que quelques-uns, proposent déjà aux entreprises et aux particuliers des solutions d’assurance à la pointe de la technique afin d’apporter des réponses adéquates au marché.

**Unir nos forces contre les risques**

Or, les assureurs peuvent-ils offrir une protection tout seuls ? En tant qu'association libérale, nous ne saurions réclamer de nouvelles dispositions réglementaires ni l'intervention de l'Etat. Or, nous pensons qu'il est important – surtout pour nous les assureurs – de ne pas occulter cet aspect ambivalent de la transformation numérique. Il nous faut répondre à la question de savoir si l'intervention de l'Etat est opportune, quelle forme celle-ci doit prendre et dans quels domaines les acteurs économiques peuvent définir eux-mêmes des mesures de précaution.

La distribution des rôles et l'élargissement des champs d'action de l'Etat et de l'économie doivent être clarifiés avec précision. Pour toutes ces questions, l'ASA coordonne les requêtes de l'ensemble de la branche et a constitué à cet effet un groupe de travail avec des spécialistes des sociétés membres. Le comité directeur œuvre actuellement à l'élaboration des bases de réflexion nécessaires qui s'inspirent des travaux du groupe de travail. En la matière aussi, le contact avec les autres associations sectorielles, les pouvoirs publics et les politiques est primordial. Faire cavalier seul est de moins en moins possible, surtout en matière de cyberrisques.

**Mesures de protection**

La maîtrise commune des cyberrisques repose essentiellement sur deux mesures centrales : la sensibilisation de l'opinion publique et la coopération internationale à tous les niveaux. La prise de conscience des dangers liés aux cyberrisques est très lacunaire et est clairement perfectible. Il nous faut sensibiliser en conséquence l'opinion publique – et en particulier les PME. En matière de lutte contre la cybercriminalité, l'union des forces s'impose. Les cyberrisques ne s'arrêtent pas aux frontières. Les cybercriminels doivent pouvoir faire l'objet de poursuites pénales systématiques, ceci au niveau international. Nous, les assureurs, nous sommes tenus de stimuler et de développer la coopération internationale entre nous et avec les autorités compétentes. Je pense surtout à des statistiques communes sur les dommages et à une gestion de crise bien organisée.
Par ailleurs, il faudrait étudier l'opportunité de la mise en place d'une cellule centralisée dédiée au signalement des cyberincidents.