Les menaces cyber dans le secteur maritime: a-t-on déjà envisagé tous les scénarios ?

L'industrie maritime est en pleine mutation grâce à sa dépendance accrue des nouvelles technologies. Aujourd'hui, les opérations de transports maritimes sont inconcevables sans l'internet, les systèmes d'aide à la navigation, embarqués ou satellitaires, et sans les différentes liaisons de communication reliant les navires aux ports.

Cette dépendance accrue des nouvelles technologies a eu immédiatement pour conséquence la recrudescence de la menace cyber. Comme partout ailleurs, l'industrie maritime a enregistré plusieurs attaques cyber majeures durant les trois dernières années, dont certaines ont entraîné des conséquences financières de l'ordre de milliards de dollars pour les compagnies d'assurances. On en retiendra en particulier, dans le transport maritime, la très récente attaque de la mi-avril 2020 contre les centres de données du groupe MSC, à Genève, qui a contraint le groupe à restreindre l'accès à son site internet pendant quelques jours. En 2018, plusieurs attaques ont été enregistrées dont celle contre le groupe chinois Cosco dans le port de Long Beach le 24 juillet 2018, celle contre le port américain de San Diego en octobre de la même année. En 2017, le groupe AP Møller-Maersk a été la cible de l'attaque du *NotPetya*, qui a, par ailleurs, touché certains ports de commerce dont ceux de Rotterdam, de New York et Mumbai. Cette attaque aurait coûté plus de 300 millions de dollars à Maersk et détruit des dizaines de milliers d'ordinateurs lui appartenant; au total, 4000 serveurs, 45000 ordinateurs et 2500 applications ont été détruits. Dans la même année, l'attaque du *WannaCry*, intervenue quelques mois plus tôt, a coûté à l'ensemble des opérateurs économiques de la planète plusieurs milliards de dollars.

Beaucoup de ces attaques ont montré que le risque cyber est de nature systémique, à cause de sa capacité à affecter un nombre important d'entreprises simultanément. Mais certains scénarios étudiés montrent que des évènements cyber peuvent entrainer des conséquences beaucoup plus graves que celles qu'on a connues jusqu'à présent.

Des scénarios de cyber attaques systémiques plus importantes

Des études réalisées via le projet *Cyber Risk Management (CyRiM)* dirigé par l'Université technologique de Nanyang au Singapour, en collaboration avec des partenaires industriels et universitaires, notamment le *Cambridge Center for Risk Studies, ont exploré* deux scénarios d'attaques cyber, le *Shen Attack* et le *Bashe Attack*, pour mettre en évidence les conséquences d'une cyber attaque systémique de grande ampleur sur l'économie globale et le marché de l'assurance.

L'un, le scénario du *Shen Attack*, a porté sur le secteur maritime et l'autre, le *Bashe Attack*, présenté de façon abstraite, sans précision d'un secteur spécifique, offre une vision générale de ce que pourraient être les conséquences d'une infection généralisée à travers un maliciel contagieux. Ce dernier scénario a mis en évidence des pertes et dommages potentiels, à

l'échelle mondiale, allant de 85 à 193 milliards de dollars, dont 10 à 27 milliards de dollars pour le marché de l'assurance.

Nous nous intéressons, pour notre analyse, au scénario du *Shen Attack*.

Ce scénario décrit trois hypothèses d'attaque cyber sur les systèmes informatiques d'une société de gestion de flottes de navires ayant des connexions avec les plus grands ports de la région Asie-Pacifique, fréquentés par les navires qu'elle a à charge. Notons que les sociétés de gestion de flottes assurent une grande variété de services au profit des armateurs, comprenant la mise à disposition d'équipages, des inspections techniques, l'organisation des voyages etc. Elles peuvent avoir à gérer des flottes de plusieurs centaines de navires. Par exemple le géant mondial du *shipmanagement*, V.Group, tient une flotte de 940 navires à travers 30 pays dans le monde.

L'objectif du *Shen attack* est de mettre en évidence les impacts d'une attaque cyber systémique sur l'économie mondiale et le niveau du marché de l'assurance cyber dans le secteur maritime.

Les systèmes informatiques de la société de gestion de flottes de navires ont été infectés par un virus. Le virus se propage et affecte tous les navires de la flotte en activité. Il s'est ensuite étendu, grâce aux liaisons de communication, à tous les ports fréquentés après par les navires infectés. Cette propagation étendue du virus a été possible dans la mesure où désormais, beaucoup d'échanges de données entre navires et ports fréquentés s'effectuent par voie électronique. La propagation du virus dans les ports a entraîné leur fermeture.

Le scénario est imaginé sur quelques-uns des ports les plus actifs au monde, et qui se trouvent pour la plupart dans la région d'Asie-Pacifique. Dans une première situation, l'attaque a affecté des ports japonais, malaisiens et singapouriens. Dans une deuxième hypothèse, des ports coréens sont ajoutés à la première liste et la troisième situation, la plus extrême, a intégré les ports chinois à la liste de ceux déjà infectés. Au total 15 ports ont été touchés par l'attaque et ont tous dû être fermés.

Impacts du scénario du *Shen Attack*

Les pertes économiques totales subies, directement ou indirectement, du fait de l'attaque, sont estimées, pendant la période de fermeture des ports, à 40.8 milliards de dollars dans la première situation, 55.9 milliards de dollars dans la deuxième et 109.8 milliards de dollars dans la troisième. Le nombre de conteneurs touchés est évalué, en evp, respectivement à 1.2 million,1.43 million et 3.69 millions.

Les pertes directes sont constituées des dommages aux marchandises périssables, du fait de l'attaque cyber, mais également de ceux qui résultent de la fermeture des ports, tandis que les pertes indirectes sont essentiellement liées à la suspension de la production et des exportations.

Pour les assureurs, trois types de couvertures sont en cause : les polices cyber ordinaires qui couvrent les pertes de données, les responsabilités, les dommages aux biens et d'autres pertes résultant de la défaillance des systèmes de communication, accidentel ou non; les polices ordinaires qui contiennent une clause d'exclusion des risques cyber, qui pourraient cependant être affectées parce que la clause n'est pas, par exemple, suffisamment précise ou complète pour exclure toutes les conséquences potentielles d'une attaque cyber ; le troisième type de couvertures regroupe les polices d'assurances mentionnées ''tous risques'' qui ne comportent aucune exclusion expresse des risques cyber. En cas de cyber attaques, en plus de la première catégorie de couvertures qui devra naturellement être mise en œuvre, les deux dernières vont aussi l'être, pour ce qu'il est convenu d'appeler ''couverture silencieuse'' ou *le cyber silent cover*.

Dans le scénario du *Shen Attack*, les pertes subies, en dollars, par l'industrie de l'assurance dans les trois situations envisagées sont respectivement de 3.64 milliards; 4.98 milliards et 8.29 milliards. La part du marché cyber ''assumé' représente respectivement 1.39 milliard; 1.94 milliard et 3.60 milliards (soit 38%; 39%; 43%) et les garanties silencieuses (*cyber silent cover*), 2.26 milliards; 3.03 milliards et 4.73 milliards (soit 62%, 61%, 57%).

Dans la situation la plus extrême, où les pertes enregistrées par le secteur de l'assurance, sont de 8.29 milliards de dollars, sur une perte globale de 109.8 milliards de dollars, occasionnées par l'événement, on constate que 92% de ces pertes ne sont pas assurées. La part assurée est répartie comme suit: 43% des pertes subies par les assureurs, sont couvertes par des polices cyber et 57% sont des garanties silencieuses.

Des opportunités à explorer pour le marché de l'assurance

Le scénario du *Shen Attack* montre que la quasi-totalité des secteurs d'activités sont exposés, au moins par ricochet, aux effets des attaques cyber systémiques. Il a montré que des secteurs comme la santé, l'agriculture, l'énergie, la pharmacie, le tourisme, la vente au détail, la construction, l'immobilier etc, ont été touchés. Les pertes subies par l'ensemble de ces secteurs que l'on peut considérer comme des victimes collatérales, sont comprises entre 0,7 milliards et 28,2milliards de dollars. Le marché de l'assurance pourrait donc explorer cette diversité de clientèles potentielles.

Par ailleurs, le marché cyber peut étendre le champ des couvertures cyber à la Responsabilité Civile des Dirigeants et des Administrateurs, la garantie ''D&O'', pour couvrir la responsabilité personnelle des chefs d'entreprises. En effet, dans le contexte actuel où la digitalisation transforme les savoir-faire traditionnels, les dirigeants peuvent, parfois, faire des choix qui ne fonctionnement pas; ou bien un sinistre survient parce qu'ils ont commis des erreurs dans la prise des décisions, ou omis d'agir au mieux des intérêts de l'entreprise, des salariés et des actionnaires. Par exemple, en matière cyber, le dirigeant n'a pas adopté les mesures de cyber sécurité appropriées. Des événements aussi graves que le *Shen Attack* pourraient conduire des actionnaires à demander des comptes à l'organe de direction, mettant ainsi en cause sa responsabilité, en raison par exemple, d'un défaut de plans de préparation, et potentiellement d'une mauvaise mise en œuvre des plans de préparation, favorisant ou aggravant le sinistre. La garantie ''D&O'' pourra alors, ici, trouver tout son intérêt.

Pourquoi la proportion des garanties silencieuses est-elle si importante ?

On parle de garanties silencieuses (*non-affirmative cyber cover*, ou *silent cyber cover*) toutes les fois qu'une police qui n'a pas expressément prévu la couverture d'un risque cyber, ou ne l'a pas expressément exclu, ou l'a mal ou insuffisamment exclu, se trouve à être mise en œuvre pour des réclamations relatives aux conséquences d'un évènement cyber, lorsque les dommages subis sont considérés comme faisant partie de ceux couverts par la police.

La proportion des garanties silencieuses dans le scénario du *Shen Attack*, représente dans les trois situations présentées, 62%, 61%, 57% contre 38%; 39%; 43% représentant celle des couvertures cyber souscrites. La raison de cette disproportion est que le marché cyber est encore très restreint et les garanties silencieuses, par définition, découlent généralement des polices ''tous risques'' qui n'ont pas dû exclure les risques cyber, ou les ont insuffisamment ou mal exclus. Ensuite dans un scénario de cyber évènement systémique, la part des polices ''tous risques'' touchées peut être rapidement importante en quantité.

Pour ceux des assureurs qui ne sont pas encore prêts pour affronter des risques cyber, ni expressément ni par le biais de couvertures silencieuses, la question des garanties silencieuses

reste une véritable problématique. En plus de la nécessité de faire davantage attention au contenu des clauses d'exclusion des risques cyber, il serait peut-être indispensable de les inclure dans toutes les polices ''tous risques '', même dans les cas les plus improbables.

ADAM ASSURANCES –33, Allées de Chartres – 33000 Bordeaux
www.adam-assu-mar.com
*Le **Lab*** – Recherches et innovations en assurances maritimes et transport
En partenariat avec le Centre de droit maritime et océanique, Nantes et le Centre de recherche et de documentation européennes et internationales, Bordeaux
Patrice A. EDORH-KOMAHE
pedorh-komahe@adam-assu-mar.com

Publié le 20 avr. 2020.