LES « CYGNES NOIRS » : CES ÉVÉNEMENTS INATTENDUS DANS LES PORTS ET LES TERMINAUX

Les ports et les terminaux sont une composante essentielle des infrastructures d'un pays ou d'une région. Même si les exploitants peuvent avoir connaissance des risques complexes auxquels ils sont exposés et emploient les pratiques exemplaires pour les atténuer, ils ne sont peut-être pas pleinement préparés aux conséquences potentiellement désastreuses d'un événement peu probable, mais dont l'incidence est grave. Un tel événement rare, comme une catastrophe naturelle, un acte de terrorisme ou la guerre, ou même une cyberattaque majeure, qu'on ne peut entièrement prévoir ou atténuer, est ce que l'on appelle un « cygne noir ».

LES CYGNES NOIRS ET LES PORTS ET TERMINAUX

Les catastrophes naturelles qui frappent les ports et les terminaux ne sont pas entièrement imprévues et peuvent, à divers degrés, être atténuées. Toutefois, certains événements moins fréquents, mais plus extrêmes – qu'on appelle aussi des événements « cygnes noirs », sont beaucoup plus difficiles à prédire, et par conséquent, à gérer. Des catastrophes naturelles majeures telles qu'un tremblement de terre, l'activité volcanique, une tempête de vent, une inondation ou un tsunami peuvent causer des dégâts considérables dans les ports et les terminaux. De plus, une attaque terroriste ou une cyberattaque à grande échelle pourraient occasionner un événement cygne noir.

L'identification des risques, des pratiques exemplaires de contrôle et la préparation aux interventions en cas d'urgence n'ont rien de nouveau pour les propriétaires et les exploitants de ports et de terminaux, mais un événement cygne noir ne compte peut-être pas parmi ceux pour lesquels on établit généralement un plan d'action. La nécessité d'une gestion des risques rigoureuse est augmentée par le fait que les ports et les terminaux sont généralement des infrastructures critiques à l'échelle nationale ou régionale, dont les activités sont essentielles tant pour la stabilité économique que politique.

Un événement cygne noir ne cause pas nécessairement des dommages directs à l'infrastructure d'une entreprise portuaire, mais il pourrait nuire de façon catastrophique à l'exécution d'activités pour le compte de clients clés. Ainsi, l'événement a le potentiel de miner la confiance des investisseurs ou de détruire des réputations.

SPOTLIGHT

Qu'est-ce qu'un « cygne noir »?

Tel que Nassim Nicholas Taleb l'écrivait dans son livre publié en 2007, The Black Swan[1], de tels événements extrêmes revêtent trois caractéristiques clés :

1. Leur probabilité est faible, compte tenu des connaissances et de l'expérience acquises.
2. Même s'ils sont peu probables, ils ont des conséquences dévastatrices lorsqu'ils se produisent et causent un choc profond.
3. Il est impossible de prédire la nature exacte de l'événement, mais rétrospectivement, il est défini comme ayant été une préoccupation évidente que l'on aurait dû ou pu mieux comprendre et, dans une certaine mesure, pressentir comme un risque potentiel.

De plus, les cygnes noirs pourraient être aggravés par la survenance simultanée d'événements à risque, peut-être en raison d'hypothèses indéterminées ou erronées.

[1] Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable,* New York: Random House, 2007.

LES PORTS ET LES TERMINAUX PRÉSENTENT DES PROFILS DE RISQUES UNIQUE

Les ports et les terminaux sont exposés à une gamme complexe de risques pendant la manipulation et le stockage des marchandises et la gestion du transport sécuritaire de celles-ci ainsi que, dans certains cas, du transport de passagers.

En plus de présenter des risques pour la sécurité des biens et des passagers qui y transitent, un port peut être exposé à des risques d'interruption des activités et à une baisse correspondante de revenus découlant de nombreux facteurs qui échappent à son contrôle. Cela peut comprendre le refus de l'accès au port si une voie d'accès essentielle par mer, par route ou par rail est bloquée ou endommagée, ou en cas de dommages aux installations d'un partenaire clé comme une mine, une usine, un entrepôt, ou un port. Cela peut également comprendre les conséquences d'une panne des services publics essentiels ou une cyberattaque.

Compte tenu du risque d'interruption des activités, les conséquences d'un événement cygne noir sur les ports et les terminaux pourraient être graves et les exploitants doivent les examiner de plus près dans le cadre de la gestion de leurs risques.

ÉTUDES DE CAS

Explosion dans le port de Tianjin

Le 12 août 2015, le port de Tianjin, en Chine, a été secoué par une explosion qui a projeté une boule de feu et une onde de choc dans tout le site, provoquant l'explosion des conteneurs d'expédition et de véhicules qui se trouvaient dans la zone portuaire et sur un viaduc autoroutier avoisinant. Cette explosion a provoqué la destruction d'entrepôts, d'installations de production et de dortoirs, frappé la gare Donghai Road située tout près, et soufflé les fenêtres de structures résidentielles sur plusieurs kilomètres.

Cet événement, qui a frappé le dixième plus important port au monde, est devenu l'un des sinistres d'origine humaine les plus considérables et complexes de l'histoire récente. Les conséquences de ce sinistre ont été ressenties bien au-delà de la zone portuaire comme telle, car il a perturbé des chaînes d'approvisionnement dans le monde entier, sans compter l'incidence qu'il a eue sur l'industrie automobile. D'aucuns s'attendent à ce que l'effet de cette explosion sur les chaînes d'approvisionnement sera de très longue durée.

Il ressort de certains rapports que l'explosion avait été causée par des produits chimiques dangereux stockés dans l'un des entrepôts. Mais même si l'on peut faire valoir que des précautions auraient pu être prises pour atténuer ce risque, de par son ampleur pure et simple, les dommages occasionnés par ce sinistre devraient s'élever à près de 1 milliard de dollars américains. Ces dommages, combinés à la complexité des chaînes d'approvisionnement modernes, signifient que ce sinistre aura des résultats imprévisibles pour l'industrie maritime.

Selon Guy Carpenter, l'indemnisation finale des dommages assurés découlant du sinistre de Tianjin pourrait être de l'ordre de 874 millions de dollars américains. Ce chiffre englobe les pertes considérables subies par l'industrie automobile et des pertes de marchandises de plusieurs millions de dollars

LE BESOIN D'ANALYSE PROSPECTIVE ET DE COORDINATION ENTRE LES PARTIES PRENANTES

Même s'il est impossible de prévoir avec exactitude les conséquences d'un événement cygne noir sur les ports et les terminaux, procéder à des analyses prospectives et à la vérification des hypothèses est essentiel. Comme pour tous les risques, il convient de scruter les points de vue internes et externes afin de s'assurer qu'aucune hypothèse, lacune ou menace ne demeure inexplorée. Par exemple, même si l'on pourrait faire valoir qu'un phénomène physique comme l'éruption du volcan Eyjafjallajökull en 2010 et le nuage de cendres qui en a résulté représentaient un risque connu, les répercussions considérables de cet incident sur les voyages internationaux ne pouvaient pas être prévues, non plus qu'on pouvait s'y être préparés.

Pour les ports et les terminaux, même si les catastrophes naturelles sont un risque prévisible, certaines catastrophes peuvent avoir des conséquences dont la gravité est inattendue.

L'un de ces événements cygne noir a été le typhon Maemi qui a frappé la Corée du Sud en 2003. Ce sinistre évalué à plusieurs milliards de dollars a causé des dommages considérables dans le port de Busan, endommageant les infrastructures et les navires.

Même si la Corée du Sud est sujette aux typhons, c'est la combinaison de la force du typhon Maemi, du fait qu'il a frappé le port directement, de surcroît à marée haute, qui a donné lieu à des dommages aussi considérables.

D'autres menaces à grande échelle pourraient comprendre le manque d'infrastructures essentielles dans l'environnement portuaire, pour lesquelles on n'aurait effectué aucune analyse des répercussions sur les opérations ni aucune planification. Les exploitants de ports et de terminaux devraient être au courant de leurs principaux actifs, mais combien d'entre eux ont vérifié leurs hypothèses touchant la continuité, ou pris en compte leur dépendance envers des actifs qui n'appartiennent pas à l'entreprise?

Une cyberattaque pourrait avoir des conséquences désastreuses pour un exploitant de port ou de terminal. À peu près jusqu'en 2010, la majorité des cyberattaques étaient motivées par l'intention d'obtenir des renseignements personnels ou des données financièrement sensibles. À l'heure actuelle, la nature de la menace est en mutation, les sociétés de tous les secteurs d'activités ont fait l'objet de cyberattaques très sophistiquées et complexes qui visent à endommager les biens et les opérations en cherchant à prendre les commandes de systèmes de contrôle industriel.

Les actifs et les infrastructures portuaires peuvent également être exposés à des actes de violence motivés par des considérations politiques liées à des grèves, à des émeutes, à des troubles civils, au terrorisme ou à du sabotage. Les menaces que représentent ces événements sont peut-être bien comprises, mais les risques qu'elles représentent changent.

Considérons, par exemple, une menace selon laquelle on aurait caché un dispositif nucléaire, une bombe radiologique ou une bombe conventionnelle dans un conteneur. Même s'il n'y avait aucune arme en réalité, la menace à elle seule pourrait entraîner la fermeture du port pendant qu'on procéderait à une recherche laborieuse dans des milliers de conteneurs.

Les exploitants de ports et de terminaux devraient élaborer des plans d'urgence contre le risque que des terroristes ou un État-nation piratent et perturbent les systèmes de navigation électronique qui permettent l'accès au port dans l'intention d'interrompre le commerce avec le pays ou la région.

Manifestement, des événements de ce genre pourraient avoir des ramifications considérables, sinon catastrophiques, pour les ports et les terminaux, et les exploitants devraient envisager la possibilité que des événements extrêmes se produisent et les effets que ceux-ci pourraient avoir sur leurs intérêts, tant internes qu'externes.

Lorsque possible, il est recommandé d'adopter une approche tenant compte des différentes parties prenantes, afin de comprendre le contexte commun du risque, les causes de risque et la reddition de compte partagée concernant les contrôles.

Pour faire face à une catastrophe majeure, il faut une approche adaptée tenant compte des différentes parties prenantes pour la gestion de crise, la gestion de la continuité des activités et la gestion des risques. Le ciment qui maintient le tout ensemble est formé de leadership, de gestion et d'efficacité du personnel.

COMMENT PEUT-ON GÉRER LES ÉVÉNEMENTS CYGNE NOIR?

Les événements cygnes noirs sont des sinistres de longue portée qui ne peuvent être identifiés avec précision, et il peut être difficile de mettre en place des contrôles pour en atténuer l'ampleur à un niveau jugé aussi faible que raisonnablement possible. Par conséquent, les exploitants ports et de terminaux ont besoin d'être suffisamment résilients pour pouvoir gérer de tels événements inattendus. On peut définir la résilience comme étant la capacité d'une entreprise à faire face aux perturbations imprévues de toutes origines susceptibles d'avoir une incidence sur sa stratégie ou sur les activités essentielles à sa mission (c'est-à-dire, qui ont une importance stratégique), que ces perturbations touchent ses actifs, ses employés ou ses processus.

Pour faire face à une catastrophe majeure, il faut une approche adaptée tenant compte des différentes parties prenantes pour la gestion de crise, la gestion de la continuité des activités et la gestion des risques. Le ciment qui maintient le tout ensemble est formé de leadership, de gestion et d'efficacité du personnel. La compréhension, la communication et la motivation sont des conditions préalables pour une performance de haut niveau pendant une situation de crise.

Il faut examiner régulièrement les activités essentielles à la mission, et combiner les plans de continuité des activités et d'intervention en cas de crise et les mettre en pratique aux niveaux stratégique et tactique pour s'assurer d'avoir la résilience et la souplesse nécessaires pour intervenir. Ce serait une erreur de supposer que la résilience équivaut à la continuité des activités, cette dernière étant gérée à un niveau opérationnel. Si un événement extrême devait se produire, ses répercussions se feraient sentir dans l'ensemble de la société d'exploitation portuaire, et les mesures prises par la haute direction seraient examinées de près et rapportées 24 heures sur 24, 7 jours sur 7 par tous les canaux de communication.

LE RÔLE DE L'ASSURANCE LORS D'UN ÉVÉNEMENT CYGNE NOIR

Bien que les polices d'assurance responsabilité patronale, responsabilité civile, dommages matériels et perte d'exploitation seront invoquées dans le cas d'une « perte normale », l'assurance ne doit jamais être considérée comme un moyen complet de traitement des risques. De plus, la protection d'assurance contre les risques cygnes noirs est loin d'être simple. Sous sa forme traditionnelle, l'assurance est limitée en termes de couverture, propre à des risques pris individuellement, et lente à indemniser. Après un sinistre, une entreprise peut ne disposer que d'une très courte période, soit quelques semaines ou même seulement quelques jours, pour persuader les milieux financiers, les créanciers, les organismes de réglementation et les gouvernements qu'elle a suffisamment de liquidités pour traverser la crise de manière ordonnée.

Il est donc nécessaire, pour les ports et les terminaux, de disposer de solutions d'assurance bonifiées pour faire face à d'éventuels événements cygnes noirs.

Pour ce faire, il faut des libellés de police étendus à un public élargi et un processus de règlement des sinistres faisant appel à des déclencheurs paramétriques permettant le règlement des sinistres dans des délais établis selon des modalités préalablement convenues. Ces solutions complémentent une stratégie gestion et de financement des risques bien structurée, qui comprend un plan d'urgence pour les liquidités après un événement cygne noir.

Avant de créer des solutions financières, il est nécessaire de procéder à une analyse de résilience approfondie des répercussions sur l'entreprise, combinée à une analyse des assurances et de la réactivité financière. Cette analyse devrait ensuite être superposée à l'appétit pour le risque et à la tolérance au risque pour créer des solutions de financement et d'assurance sur mesure.

Il est nécessaire, pour les ports et les terminaux, de disposer de solutions d'assurance bonifiées pour faire face à d'éventuels événements cygnes noirs.

CONCLUSION

Les événements cygnes noirs présentent un défi unique pour les ports et les terminaux, tant sur le plan de la difficulté de les prévoir et de les atténuer que sur le plan des conséquences potentiellement dévastatrices qu'ils peuvent entraîner. On ne doit pas sous-estimer les risques que posent ces événements pour ces infrastructures souvent essentielles. Afin de pouvoir mieux garantir la réussite future des ports et des terminaux, il faudrait procéder à une évaluation approfondie de ce domaine clé de risque combinant des analyses prospectives, des tests de résilience, un examen des assurances ainsi que des tests d'endurance financière. Cette analyse détaillée permettra la création de contrôles plus solides, financiers ou autres, afin d'assurer la reprise durable d'un port ou d'un terminal après un événement catastrophique.

À propos de Marsh

Marsh est un chef de file mondial en courtage d'assurances et en gestion de risques. Marsh aide ses clients à prospérer en définissant, en concevant et en mettant en place des solutions novatrices et propres à leur domaine d'activités afin de leur permettre de gérer efficacement les risques. Marsh emploie environ 30 000 personnes qui travaillent en collaboration pour donner satisfaction à des clients présents dans plus de 130 pays. Marsh est une filiale en propriété exclusive des Sociétés Marsh & McLennan (NYSE : MMC), groupe mondial de sociétés de services professionnels qui offrent à leurs clients des conseils et des solutions en matière de risques, de stratégie et de capital humain. Fortes d'un chiffre d'affaires annuel de 13 milliards de dollars et d'environ 60 000 employés à l'échelle mondiale, les Sociétés Marsh & McLennan sont également la société mère de Guy Carpenter, chef de file mondial des services de gestion des risques et intermédiaire en réassurance, de Mercer, important fournisseur de services-conseils en gestion des talents, soins de santé, retraite et investissements et d'Oliver Wyman, un des principaux cabinets de services-conseils en gestion. Suivez Marsh sur Twitter, @MarshGlobal, LinkedIn, Facebook et YouTube.

À propos de ce rapport

Ce rapport a été produit par le groupe d'expertise mondial en assurances maritimes de Marsh, un chef de file des services-conseils au secteur maritime en ce qui concerne les enjeux de risque et d'assurance, qui a la réputation de partager ses connaissances et de fournir des solutions pour permettre à ses clients de relever les défis auxquels ils sont confrontés. Ce groupe d'expertise, qui comprend plus de 600 experts en assurances maritimes qui se consacrent aux services à ce secteur, gère un volume de primes d'assurance de plus de 3 milliards de dollars américains. Avec des activités dans plus de 100 pays dirigées à partir de 12 centres stratégiques, Marsh est un chef de file mondial dans le domaine du courtage d'assurances et de la gestion de risques.

Pour en savoir plus, communiquer avec :

NICK MAY

Vice-président
Groupe d'expertise mondial en assurances maritimes
44 (0)20 7357 2180
nick.may@marsh.com

EDWIN CHARNAUD

Président
Groupe d'expertise mondial en infrastructures
44 (0)20 7357 3157
edwin.charnaud@marsh.com

MARCUS BAKER

Président
Groupe d'expertise mondial en assurances maritimes
44 (0)20 7357 1780
marcus.baker@marsh.com