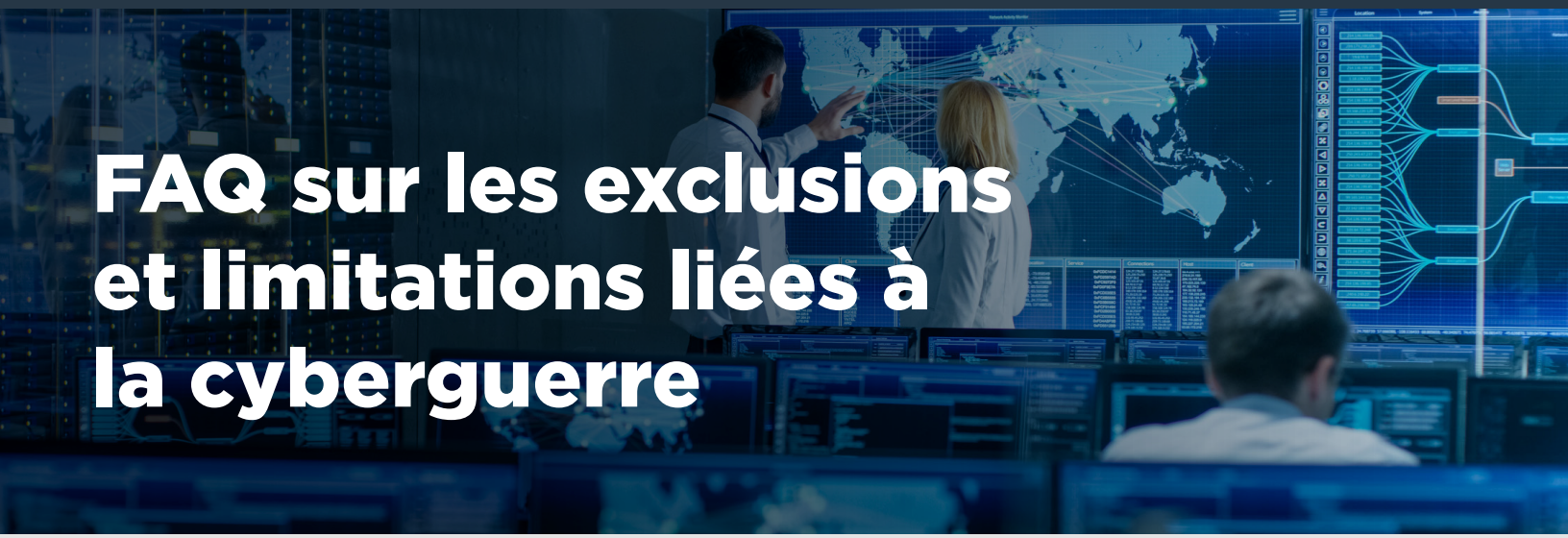

FAQ sur les exclusions et limitations liées à la cyberguerre

La cybersécurité est un défi permanent, mais les organisations ne sont pas seules pour protéger leur réseau/système informatique et leurs actifs numériques. L'équipe d'experts en cybersécurité et technologie de HUB International répond à quelques questions courantes ci-dessous:

Qu'est-ce qu'une exclusion de guerre?

Une exclusion de guerre est une clause de provision type des polices tous risques qui exclut la couverture des pertes causées par la guerre ou des actes de guerre hostiles. La clause est large (voir les exemples détaillés ci-dessous) et l'attribution est un élément clé. Les assureurs doivent fournir une attribution factuelle selon laquelle une cyberattaque a été déployée comme une arme par un gouvernement, une entité travaillant pour un gouvernement ou en lien avec celui-ci.

En raison du conflit en cours, le langage d'exclusion et les limitations de couverture potentielles dans les polices d'assurance cyber-risques sont une priorité. Il y a des questions quant aux implications possibles et si la couverture risque d'être refusée sur la base de l'exclusion de guerre si une cyberattaque censée être liée au conflit en cours entraînait une perte.

Les limitations de couverture sont importantes, car, dans le cas de la Russie, elle a lancé des attaques DDoS et des logiciels effaceurs (wiperwares) contre l'Ukraine avant son invasion, et continue de le faire après. Si le logiciel malveillant atteint les côtes nord-américaines, comme l'a fait NotPetya, les pertes pourraient être exclues sur la base de la clause d'exclusion de guerre.

Si mon organisation a mis en place une police cyber-risques, sera-t-elle couverte en cas de cyberattaque?

La plupart des polices d'assurance cyber-risques/technologiques comportent des exclusions de guerre, mais HUB a également négocié avec succès des limitations touchant le cyberterrorisme à l'exclusion de guerre.

Cependant, il n'y a pas de réponse simple à cette question. L'admissibilité à la couverture dépendra des particularités de l'événement, ainsi que des résultats des litiges qui remettent en cause les exclusions de guerre et le libellé des limitations touchant le cyberterrorisme.

Ces critères incluent notamment:

- La cyberattaque faisait-elle partie de/appuyait-elle la guerre ou faisait-elle suite à des activités cyberterroristes?
- La situation correspondait-elle à la définition de guerre telle qu'énoncée dans l'exclusion ou pourrait-on faire valoir que les limitations liées au cyberterrorisme s'appliquent?

  Les réponses à ces questions ont tendance à être plus complexes parce que le libellé de l'exclusion de guerre et des limitations liées au cyberterrorisme varie selon la société d'assurance.

  Toutes les polices comportent également des exclusions de sanctions économiques pour les pays et entités qui figurent sur la liste des sanctions du Department of the Treasury and Office of Foreign Assets Control des États-Unis (OFAC). L'invasion russe de l'Ukraine est une guerre et des sanctions ont été appliquées.

  Dans le cas où une société d'assurance refuserait d'honorer une réclamation invoquant l'exclusion de guerre, il est probable que cela ferait l'objet d'un procès approfondi devant les tribunaux pour déterminer si la couverture devrait s'appliquer pour un cyberévénement lié au conflit en cours en Russie/Ukraine.

  De plus, si un assuré était victime d'une cyberattaque provenant de Russie, il incomberait à l'assureur de démontrer clairement que le cybercriminel russe agissait au nom du gouvernement.

Qu'est-ce qu'une exclusion liée aux sanctions?

Les sanctions, ou les peines imposées par un pays à un autre pour activité hostile ou violation du droit international, sont parmi les actions les plus préjudiciables que les nations puissent entreprendre, à moins d'aller à la guerre.

Une exclusion de sanction couvre toute sanction imposée par les Nations Unies, ainsi que celles imposées par les États-Unis, le Royaume-Uni et l'Union européenne.

À ce jour, plus de 5500 sanctions ont été imposées à la Russie, y compris à des entreprises et des particuliers, comme les riches oligarques proches du Kremlin.

Dans certaines circonstances, l'exclusion de sanction peut interdire le paiement des demandes d'extorsion ou de rançongiciel.

Au cours des deux dernières années, les assureurs ont commencé à refuser de payer (ou de rembourser les assurés pour le paiement) des demandes d'extorsion aux cybercriminels/gangs de rançongiciels qui figurent sur la liste de l'OFAC, qui ne cesse de s'allonger, ou à cause de la directive de février 2022 de l'OFAC. Par exemple, alors que Conti (un gang de rançongiciels favorable à la Russie) ne figure pas sur la liste de « non-paiement » de l'OFAC, le paiement à Conti est interdit en raison de la directive de l'OFAC.

Les responsables de la menace évoluent constamment, changeant leurs méthodes d'attaque et leurs noms pour échapper à la loi.

À l'heure actuelle, les attaques de DDoS et de logiciels effaceurs sont les principales méthodes d'attaque. Cependant, cette exclusion pourrait survenir si un événement lié à un rançongiciel se produisait et qu'il était déterminé qu'il avait été initié par des groupes ou des individus sanctionnés. (Par conséquent, le paiement d'une rançon serait interdit à ces groupes ou individus.)

Quels types d'attaques sont possibles?

La Russie déploie des cyberarmes de guerre de qualité militaire et utilise des logiciels d'essuyage destructeurs de réseaux. Bien que les attaques aient été ciblées jusqu'à présent, certaines de ces armes sont des vers conçus pour se propager à l'intérieur et à l'extérieur des réseaux cibles, notamment :

- WhisperGate
- HermeticWiper
- IsaacWiper
- Ransomware gangs siding with Russia
    - Conti
    - Lockbit

Encore une fois, ce scénario n'est pas nouveau.

En 2016, la Russie a attaqué l'Ukraine avec DDoS et un logiciel effaceur. Une arme, NotPetya, visait à terroriser les Ukrainiens. Implanté sur un site de logiciel fiscal utilisé par 85 % des citoyens du pays, le logiciel malveillant a effacé les systèmes informatiques des utilisateurs et s'est propagé à d'autres. NotPetya s'est ensuite propagé au reste du monde, créant une cyberpandémie qui a entraîné d'énormes problèmes d'interruption d'activité, ainsi que des pertes de biens aux États-Unis.

NotPetya et le logiciel malveillant WannaCry de la Corée du Nord ont été construits sur une cyberarme perdue de la National Security Agency (NSA) appelée Eternal Blue. Ces logiciels effaceurs sont extrêmement difficiles à éliminer de par leur conception. Certaines entreprises ont passé plus d'un an à les combattre, tandis que de nombreuses autres ont dû éliminer définitivement les ordinateurs, périphériques et équipements réseau infectés. Par la suite, les administrateurs et dirigeants de certaines entreprises ont été poursuivis en justice pour des divulgations et des délits d'initiés.

Quelle est la différence entre le terrorisme et un acte de guerre en ce qui concerne l'exclusion d'une police d'assurance cyber-risques?

Bien que le libellé utilisé dans les polices au sujet des exclusions de guerre varie selon l'assureur, l'intention est d'exclure les pertes résultant d'actes de guerre. De même, il n'y a pas d'uniformité de formulation pour les limitations négociées au sujet du cyberterrorisme; cependant, l'intention est de rembourser les pertes liées au cyberterrorisme. Ainsi, la définition entre le terrorisme et un acte de guerre sera différente selon la police.

Le cyberterrorisme est souvent défini comme des attaques ou des actes d'intimidation contre un système ou un réseau informatique motivés par la politique, la religion ou l'idéologie.

Dans de nombreux cas, NotPetya a été considéré comme un événement déclencheur en raison du libellé des limitations liées au cyberterrorisme, et donc payables en vertu de certaines polices d'assurance cyber-risques. Pour les autres types de polices, un litige a été nécessaire pour rendre une décision. Certains assurés ont cherché à récupérer les pertes liées à l'interruption de leurs activités dans le cadre des polices couvrant les enlèvements et les rançons, qui sont conçues pour payer des rançons, et non dédommager pour une interruption. Un autre assureur a cherché à invoquer une exclusion de guerre, car il avait proposé une cyber interruption sur sa couverture de propriété.

À l'inverse, la plupart des polices d'assurance cyber-risques excluent la guerre, qu'elle soit déclarée ou non.

L'Ukraine a qualifié l'invasion de la Russie et les attaques en cours de guerre, tout comme l'OTAN et les États-Unis. La plupart des polices cyber-risques excluent également les actes de guerres; ainsi, la libération d'une cyberarme en raison d'une guerre serait probablement considérée comme telle.

N'oubliez pas que l'exclusion de guerre est extrêmement large, excluant la couverture des causes directes et indirectes de perte ou de responsabilité. Elle a également une définition globale de conflit.

Les exemples d'exclusion de guerre suivants peuvent aider à illustrer cela:

EXEMPLE D'EXCLUSION DE GUERRE	
AIG	***Découlant de, fondé sur ou attribuable à:*** ...guerre, invasion, action militaire (que la guerre soit déclarée ou non), guerre civile, mutinerie, soulèvement populaire ou militaire, insurrection, rébellion, révolution, pouvoir militaire ou usurpé, ou toute action entreprise pour entraver ces actions ou se défendre contre elles.
AXA XL	Grèves ou mouvements sociaux similaires, guerre, déclarée ou non, invasion, acte d'un ennemi étranger, guerre civile, mutinerie, coup d'État, troubles civils prenant les proportions ou équivalant à un soulèvement populaire, soulèvement militaire, insurrection, rébellion, révolution, pouvoir militaire ou usurpé, ou toute action entreprise pour entraver ou se défendre contre ces actions.
London	Grèves ou actions similaires du travail, guerre, invasion, acte d'un ennemi étranger, hostilités ou opérations de guerre (déclarées ou non), guerre civile, mutinerie, agitation civile prenant les proportions ou équivalant à un soulèvement populaire, soulèvement militaire, insurrection, rébellion, révolution, militaire ou usurpée, pouvoir, ou toute action entreprise pour entraver ces actions ou se défendre contre elles. Le libellé des exclusions de guerre, ainsi que les limitations liées au cyberterrorisme, sont susceptibles de changer à l'avenir. À l'heure actuelle, HUB n'a vu aucune position affirmative sur la modification du libellé des exclusions touchant la guerre ou des limitations liées au cyberterrorisme, mais il y a un examen approfondi entourant cette formulation en ce qui concerne les futures conditions générales des polices.

SHIELDS UP: Résilience grâce à l'examen, aux ressources et à la réponse:

La Cybersecurity and Infrastructure Security Agency (CISA) a publié des conseils pour toutes les entreprises dans le cadre de sa campagne Shields Up. On y retrouve des recommandations pour les chefs d'entreprise et les PDG, des recommandations de réponse aux rançongiciels et des ressources supplémentaires sur la cyberpréparation.

Les chefs d'entreprise doivent travailler avec leurs équipes informatiques pour s'assurer qu'ils prennent les mesures nécessaires pour améliorer leur position en matière de cybersécurité et se préparer à répondre au contexte actuel des menaces à mesure qu'il continue d'évoluer. C'est peut-être aussi le bon moment pour tirer parti des ressources ou des services de prévention des attaques disponibles auprès de votre société d'assurance.

Les spécialistes en cyber-risques et technologie de HUB peuvent vous aider de différentes manières, en fournissant notamment:

- Plans de continuité d'activité
- Planification de la réponse aux incidents cybernétiques
- Recommandations des fournisseurs pour les audits de sécurité de l'information
- Examen approfondi des polices existantes
- Experts dédiés à la réponse aux violations de la technologie et à la cybersécurité et aux réclamations

HUB dispose des outils, de l'expertise et de l'expérience nécessaires pour aider les clients à se préparer à l'imprévu et à gérer une crise, si elle devait survenir.

Contactez votre expert en cyber-risque HUB pour plus d'informations sur la mise en œuvre des meilleures pratiques dans votre entreprise et l'assurance de votre cyber-risque.

hubinternational.com