ISSN 0123-1154 (IMPRESO)
ISSN 2500-7556 (EN LÍNEA)

SEGUROS CIBERNÉTICOS

CYBER RISKS

HENRIQUE JOSÉ M. SARAIVA LIMA[*]

Fecha de recepción: 15 de octubre 2019
Fecha de aceptación 30 noviembre 2019
Disponible en línea: 30 de diciembre 2020

Para citar este artículo/To cite this article

Saraiva Lima, Henrique José M. *Seguros cibernéticos*, 53 Rev.Ibero-Latinoam.Seguros, 161-172 (2020). https://doi.org/10.11144/Javeriana.ris53.seci

doi:10.11144/Javeriana.ris53.seci

[*] Senior Partner of the Law Firm "Saraiva Lima e Associados" - AIDA Portugal. Graduated in Law by the Universidade Católica Portugal (Lisboa) in July 1982. Attended a post-graduate course about EC Law at the Universidade Católica Portugesa (1982/83). Attorney at Law specialized in the areas of international transport law, insurance law and international contract law. Member of the "Ordem dos Advogados" (Portuguese Law Society) since 1984. Senior Partner of the Law Firm "Saraiva Lima e Associados" founded on April 1995 with offices in Lisbon and Oporto responsible for the Insurance department. Legal transport consultant for United Nations (UNCTAD). Contacto: saraivalima@saraivalima.com

RESUMEN

Los asegurados tienen problemas en saber en concreto lo que pretenden o necesitan y las aseguradoras continúan enfrentándose a grandes dificultades en concretar o prever los riesgos que pueden ocurrir. En lo que respecta a los riesgos cibernéticos no existe un histórico basado en años de experiencia que permita a las aseguradoras prever los riesgos en causa y los siniestros que puedan ocurrir de forma a crear y presentar soluciones equilibradas que satisfagan las necesidades de los clientes. Es importante que existan soluciones standardizadas pero, en determinados casos, el mercado asegurador debe ofrecer soluciones específicas que correspondan a las reales necesidades de los clientes, teniendo por base diligencias precontractuales, incluyendo un análisis riguroso de los riesgos envueltos. Estamos claramente ante una situación especial que puede traducirse en una alta frecuencia aliada a una alta severidad, lo que obliga a las aseguradoras a repensarse sus estrategias de forma a prevenir o disminuir eventuales perdidas substanciales. Los asegurados y aseguradoras luchan contra un enemigo que es invisible y que no puede ser responsabilizado por los daños causados por lo que la posibilidad de ejercicio del derecho de reembolso contra el causador del siniestro es prácticamente inexistente. Los seguros cibernéticos deben incluir coberturas a nivel de los daños propios, que puedan ser básicas o incluir coberturas complementarias, y de responsabilidad civil ante terceros, siendo que las indemnizaciones a pagar puedan alcanzar valores substancialmente altos. Las exposiciones no afirmativas (riesgos silenciosos) constituían una preocupación real para las aseguradoras en el contexto de la acumulación de riesgos en cuanto están en causa seguros en que los riesgos cibernéticos no están expresamente incluidos ni excluidos en el ámbito de cobertura de las respectivas pólizas. La resolución del problema puede pasar por la revisión o actualización de las cláusulas de las pólizas de seguro de forma a excluir expresamente los riesgos cibernéticos o, en alternativa, a incluirlos de forma clara e inequívoca con acuerdo con los asegurados y el consecuente aumento de la prima del seguro. La alternativa pasa por la resolución de los potenciales litigios en Tribunal en el sentido de saber si un determinado siniestro está (o no) incluido en el ámbito de cobertura de la póliza.

Palabras clave: riesgos cibernéticos, derecho de reembolso, riesgos silenciosos, acumulación de riesgos

ABSTRACT

The insured some difficulties in finding what they specifically intend or need and the insurers are still facing major problems in fulfilling or predicting those specific risks that may occur. There is no historic based on years of experience concerning cyber risks that allows the insurers to antecipate the risks at stake and the claims that may arise, in order to create and present balanced solutions that meets the clients' needs. It is important to have standard solutions, but in some cases the insurance market should be able to offer tailored solutions that meet the clients' real needs, through pre-contractual diligences including a thorough analysis of the risks involved. We are clearly facing a special situation that might turn in a most frequent with high severity scenario, which forces insurance companies to rethink their strategies in order to prevent or decrease potential and substantial losses. Both insured and insurers fight against an invisible enemy that can't be held accountable for the damages caused, so the possibility to exercise a reimbursement right against the responsible is almost non-existent. Cyber insurances shall include coverage for own damages - that can be basic or include additional coverage for third party liability, once the compensation amount can be substantially high. The non-affirmative exposure (silent risks) are a real concern for the insurers within the accumulation of risks, when it comes to insurance policies that do not explicitly include nor exclude cyber risks from its scope of coverage. The solution to this problem might be to review/update the clauses from the insurance policies in order to expressly include cyber risks. Alternatively, cyber risks should be clearly included with the insured agreement and consequently increasing the insurance premium. The alternative is to settle potential disputes in court, in order to understand if a certain claim is covered by the scope of an insurance policy.

Keywords: *cyber risks, reimbursement right, non-affirmative exposure, accumulation of risks*

1. INTRODUCCIÓN AL TEMA

Como todos saben, el mundo de los seguros está en constante evolución y se enfrenta hoy a un gran desafió en esta compleja área de los seguros cibernéticos.

El mundo de internet asumió hoy proporciones gigantescas, nunca imaginadas, y es imposible prever lo que sería el impacto al desaparecer internet y lo que tendría en la vida de cada uno de nosotros.

Se estima que:

a) son enviados por día cerca de 294 billones de correos electrónicos;

b) son efectuadas por minuto a través de Google cerca de 4,89 millones de búsquedas;

c) facebook tiene cerca de 2 billones de usuarios activos;

d) cerca de 30 millones de datos son enviados por día en los sectores de los transportes, industrias y servicios;

e) son utilizados cerca de 17,5 exabites de datos en los mercados de capital;

f) son consumidos por las familias cerca de 375 megabites por día.

Como es fácil de constatar, están en causa grandes valores económicos. Un ataque cibernético a nivel global provocaría una crisis de efectos imprevisibles y consecuencias dramáticas.

Los riesgos cibernéticos están en permanente evolución y afectan a todos (Estados, organizaciones internacionales, empresas, personas, etc.) siendo cada vez más frecuentes y agresivos los ataques cibernéticos.

La instalación de sistemas de seguridad dejo de ser una opción para pasar a ser una obligación.

Sucede, además, que la solución del problema ya no pasa unicamente por la realización de inversiones a nivel de hardware/software. Véase el caso de algunos ataques recientes que ocurrieron en diferentes partes del mundo afectando a gobiernos y administraciones públicas.

Los problemas más graves que han ocurrido en el mundo son provocados por organizaciones y/o hackers muy profesionales y con gran experiencia. El problema es particularmente grave a nivel de las empresas.

Se estima que:

a) Cerca del 82% de las empresas europeas ya se enfrentaron a un ataque informático (phising y/o ransmware);

b) Más de 1/3 de las empresas que sufrieron un ataque cibernético en 2018 tuvieron perdidas superiores a 1/3 en términos de benefícios, clientes y oportunidades de negocios;

c) Más de la mitad de las empresas identifica el riesgo cibernético como el riesgo más grave al que tienen que enfrentarse en los días de hoy.

Estamos, así, ante un gran desafió para el mercado asegurador para poder presentar soluciones eficaces; pero, también ante una gran oportunidad para las empresa aseguradoras. La búsqueda de seguros contra riesgos cibernéticos ha tenido una clara tendencia para crecer principalmente a nivel de las grandes empresas.

La EIOPA – *European Insurance and Occupational Pensions Authority,* que es la autoridad europea de supervisión del sector asegurador, realizo recientemente un estudio sobre seguros cibernéticos a nivel europeo.

El objetivo principal de la EIOPA fue el de intentar entender mejor los desarrollos actuales a nivel de la estrategia de las aseguradoras, del tipo de seguros que están a ser ofrecidos y de la potencial acumulación de los riesgos que están en causa.

Las principales conclusiones de ese estudio fueron las siguientes:

1ª conclusión: existe una necesidad clara de una comprensión mas profunda de los riesgos cibernéticos por parte de las aseguradoras, de los brokers y de los clientes.

Fue constatado que las necesidades de los clientes han sido subestimadas, han habido dificultades a nivel de valoración y del tratamiento de riesgos por parte de las aseguradoras.

En verdad, los clientes todavía tienen dificultades en saber en concreto lo que pretenden o necesitan y las aseguradoras enfrentan grandes dificultades en concretar o prever los riesgos que pueden ocurrir.

2ª conclusión: la mayor parte de los seguros existentes en el mercado tienen como destinatarios las empresas, pero el interés en contratar seguros cibernéticos dirigidos a personas empiezan a surgir una vez que los consumidores están cada vez más expuestos a la violación de los servicios digitales.

Se admite que los riesgos para las personas no sean tan graves y que las indemnizaciones a pagar en caso de siniestro no sean tan elevadas, pero lo cierto es que las personas no están libres de ser victimas de un ataque informático.

3ª conclusión: el sector asegurador cuenta con el aumento gradual de la demanda de seguros cibernéticos en consecuencia de una mayor concientización de los riesgos, de una mayor frecuencia de eventos cibernéticos y de la publicación de la nueva regulación a nivel nacional y europeo.

Es por tanto evidente, que la importancia y el número de los seguros cibernéticos a nivel global va a aumentar significativamente en los próximos años.

4ª conclusión: la falta de estadisticas es un obstáculo muy importante para la construcción de modelos matemáticos que puedan ser usados confiablemente por las

aseguradoras para construir estimados a nivel de precios, de las coberturas y de los riesgos acumulados.

En la mayor parte de los seguros existe un histórico basado en años de experiencia que permiten a las aseguradoras prever los riesgos en causa y los siniestros que puedan ocurrir de forma a crear y presentar soluciones equilibradas que den satisfacción a las necesidades de los clientes; ahora, no existe histórico en el que diga respecto a los riesgos cibernéticos.

La falta de suscriptores especializados también apunta en el estudio como un obstáculo para el desarrollo de la industria aseguradora en este área y el aumento de ofertas de pólizas de seguros con coberturas adecuadas.

Fue también constatado que exposiciones del tipo no afirmativas propician acumulaciones de riesgos.

5ª conclusión: existe una necesidad de regulación que, podría ayudar a resolver algunos de los desafíos que se colocan a la actividad aseguradora.

Las conclusiones de este estudio podran ser el punto de partida para llamar la atención para diversos problemas que se ponen en esta específica y compleja área de los seguros cibernéticos.

2. EN RELACIÓN A LA DEFINICIÓN DEL RIESGO CIBERNÉTICO

La IAIS – *International Association of Insurance Supervisors* presentó en 2016 una definición de este concepto. El riesgo cibernético fue definido como cualquier tipo de riesgo proveniente del uso de herramientas electrónicas, como internet y las redes de telecomunicaciones.

Están también incluidos en este concepto:

a) el riesgo de daños físicos que puedan ser causados por ataques cibernéticos;

b) el riesgo de fraude resultante de uso indebido de datos;

c) cualquier responsabilidad que transcurra del almacenamiento y transferencia de datos;

d) la disponbilidad, integridad y confidencialidad de las informaciones electrónicas, relacionadas con individuos, empresas y gobiernos.

Se cuestiona si esta definición continua actual y, más en concreto, si no existieran situaciones nuevas o riesgos añadidos, que fueran surgiendo en consecuencia de los ataques informáticos que haya surgido en todo el mundo, que justifiquen una actualización o ampliación del concepto.

En verdad, existe hoy en día un nuevo lexico que ha de tenerse en consideración cuando hablamos de ciberriesgos: *ransomware, spear-pishing, botnet, privacy by design ou by default, cryptocurrencies, etc*.

La definición de riesgo cibernético permite identificar las situaciones que deben ser previstas en una póliza de seguro. El ámbito de cobertura de las pólizas de seguro tiene que ser delimitado teniendo en consideración no sólo los riesgos seguros sino también las exclusiones previstas, siendo que algunas de ellas podrán ser objeto de una garantía adicional o complementaria.

Al nivel de las empresas están esencialmente en causa cinco situaciones diferentes:

a) la intromisión de terceros en los sistemas informáticos;

b) la cobertura de rescates por ransomwares;

c) el incumplimiento del deber de custodia de datos de carácter personal;

d) las responsabilidades informáticas del asegurado;

e) la violación del derecho al honor e intimidad personal de tercero.

Respecto a las personas, existen otras situaciones importantes de las cuales pueden resultar perjuicios y responsabilidades. El fraude informático puede traducirse en un robo de identidad con todas las consecuencias de ahí resultantes.

Conforme resulta del estudio realizado por la EIOPA el mercado asegurador ha tenido dificultades en presentar propuestas de seguro que tengan en cuenta la especificidad y las necesidades concretas de cada seguro. Como es evidente y ya fue mencionado, la falta de datos ha contribuido para esas dificultades.

Es indiscutible que tienen necesariamente que existir soluciones standarizadas pero no es menos verdad que, en determinados casos, el mercado asegurador debe ofrecer soluciones específicas que correspondan a las reales necesidades de los clientes.

En esa perspectiva, los brokers tienen aquí un papel fundamental por estar, en principio, más próximos y conocer mejor la realidad de los clientes, potenciales interesados en la contratación de un seguro cibernético.

La realización de diligencias pre-contractuales, incluyendo un análisis riguroso de los riesgos envueltos, especialmente cuando están en causas de empresas de gran dimensión o empresas que independientemente de su dimensión, actúan en nichos de mercado con características muy especiales.

3. EN RELACIÓN A LOS SINIESTROS

El aumento y la gravedad de los ataques cibernéticos ha puesto en causa los principios que presiden la gestión de las carteras de seguros.

Estamos claramente ante una situación especial que puede traducirse en una alta frecuencia aliada a una alta severidad, lo que obliga a las aseguradoras a repensar sus estrategias de forma a prevenir o disminuir eventuales perdidas substanciales.

Es verdad que muchos de los riesgos nacen de los propios usuarios pero los siniestros más graves son provocados por ataques informáticos efectuados por organizaciones internacionales altamente profesionales o por *hackers* bastante competentes.

Estamos en el dominio de la ciberdelicuencia y los delitos son practicados con el objetivo de obtención de importantes ventajas patrimoniales o financieras. El autor del delito puede estar actuando por cuenta propia o haber sido contratado para el efecto, como sucede en los casos de espionaje industrial y de competencia desleal.

Contrariamente a lo que sucede en la mayoría de los siniestros provocados por la acción humana que ocurren cuando esta en causa otro tipo de seguros, es el caso de los seguros cibernéticos, los autores de los delitos raramente son identificados y localizados. Los asegurados luchan contra un enemigo que es invisible y que no puede ser responsabilizado por los daños causados.

Es prácticamente ineficaz, en el caso de los seguros cibernéticos, el principio según el cual la aseguradora que hubiera pagado una indemnización queda sub-rogada, en la medida del importe pago, en los derechos del asegurado contra el tercero responsable por el siniestro. Dicho de otras palabras, la posibilidad de ejercicio del derecho de reembolso contra el causador del siniestro es prácticamente inexistente.

En la mayor parte de los ataques informáticos la presentación de una denuncia no pasa de una mera formalidad burocrática sin ningún efecto útil, dado que los proceso son invariablemente archivados por no ser posible identificar el autore del delito.

4. EN RELACIÓN A LAS COBERTURAS

Los seguros cibernéticos deben incluir coberturas a nivel de daños propios y de la responsabilidad civil ante terceros.

De un ataque cibernético puede resultar una interrupción de la actividad de la empresa con consecuencias a nivel operativo.

Los daños resultantes del ataque cibernético pueden comprender no sólo los daños emergentes, que corresponden a los gastos que la empresa tiene que soportar para restablecer la normalidad de su funcionamiento, sino también los lucros cesantes, que corresponden a los beneficios que la empresa dejo de obtener en consecuencia de ese ataque.

La cobertura de daños propios puede ser básica o incluir coberturas complementarias. Hacen parte de la cobertura básica de una póliza de seguro cibernético normas a nivel de servicios de primera respuesta, gestión de incidentes, protección de datos, interrupción de redes, incidentes de datos electrónicos, extorsión cibernética, etc.

En lo que respecta a las coberturas complementarias podemos incluir las referentes a cyber delitos, *telefone hacking, website hacking, etc.*

Más importante que la cobertura de daños propios es ciertamente la cobertura a nivel de responsabilidad civil ante terceros.

Esta encausa la responsabilidad de la empresa por violación de las normas relativas a la protección de datos personales, por el uso ilegítimo de información comercial, por la introducción de virus en los datos de terceros en el sistema informático, por la destrucción y alteración de los datos de terceros, por el hurto o pérdida de activos informáticos, por la divulgación pública de datos de terceros, por la violación de derechos de propiedad intelectual o industrial, etc.

La reglamentación europea a nivel de protección de datos personales es muy rigurosa y se ha visto gradualmente implementada en los diversos Estados miembros. La responsabilidad de las empresas en esta área es muy grande y, en caso de violación de las obligaciones que están previstas, las multas pueden llegar a valores astronómicos.

5. EN RELACIÓN A LOS SEGUROS EN VIGOR

Hay problemas graves relativamente a pólizas de seguros multiriesgos, riesgos patrimoniales y de responsabilidad civil que están en vigor hace muchos años.

Están en causa los seguros en que los riesgos cibernéticos no fueron debidamente identificados o tarifados. Se trata de riesgos denominados "implícitos" o "silenciosos" que no están expresamente previstos en la cobertura de la póliza ni expresamente excluídos de la misma.

Estamos principalmente hablando de pólizas que fueron emitidas en un momento en que no eran conocidos los riesgos cibernéticos o no existía una concientización clara, por parte de las personas y de las empresas, acerca de la importancia de estos riesgos.

Todo lo que está incluido en los seguros multiriesgos, riesgos patrimoniales y de responsabilidad civil puede estar sujeto a "riesgos silenciosos" pero el aumento y la gravedad de los ataques cibernéticos vinieron agravar el problema y las consecuencias del mismo.

El estudio realizado por la EIOPA ya refería que las exposiciones no afirmativas constituían una preocupación real para las aseguradoras en el contexto de la acumulación de riesgos.

En verdad, estos riegos "silenciosos" pueden resultar en una acumulación de perjuicios incluidos en el ámbito de la cobertura de la póliza en consecuencia de un ataque informático. La gestión de riesgo de acumulación puede transformarse en un autentico "dolor de cabeza" para los gestores de riesgos de las empresas aseguradoras por lo que puedan estar en potenciales perdidas de valor significativo.

Se colocan aqui problemas serios no sólo en términos financiero sino también a nivel jurídico, una vez que no existen exclusiones expresas para el ciber riesgo.

La resolución del problema puede pasar por la revisión o actualización de las cláusulas de las pólizas de seguro de forma a excluir expresamente los riesgos cibernéticos o, en alternativa, a incluirlos de forma clara e inequívoca por acuerdo con los asegurados y con el consecuente aumento de la prima del seguro.

La alternativa pasa por largas discusiones jurídicas a nivel del análisis del clausulado de la póliza y por la resolución de los potenciales litígios en Tribunales en el sentido de saber si un determinado siniestro está (o no) incluído en el ámbito de cobertura de la póliza.

6. CASOS CONCRETOS

Dos ejemplos de riesgos silenciosos:

a. Seguro marítimo

Una exportadora portuguesa recibió un encargo de una empresa francesa de construcción muy conocida. No era la primera vez que la empresa portuguesa proveía cables eléctricos para esta empresa francesa.

El encargo fue realizado por el director general de la empresa francesa y todos los contactos fueron efectuados por correo electrónico El valor de los cables eléctricos ascendía a más de 250.000,00 €. El contenedor con los cables eléctricos fue transportado a Inglaterra y se destinaba a unos trabajos de construcción que estaban en ejecución en este país.

La empresa exportadora contrató un seguro marítimo que garantizaba las perdidas y daños a las mercancías que pudieran ocurrir durante el transporte desde el origen hasta el destino final. El seguro tenía cobertura de almacén a almacén.

El contenedor debería ser entregado en una determinada dirección. Todavía, fueron transmitidas instrucciones al transportador para, antes de la entrega, contactar por teléfono con una determinada persona.

La persona indicada transmitió, durante la conversación telefónica, que, debido a problemas de espacio, el contenedor no podría ser entregado en la dirección inicialmente prevista, siendo indicada una nueva dirección de entrega, a (1) un km de distancia. El contenedor con la mercancía fue entregado en esa nueva dirección.

El valor de la factura no fue pago en el plazo previsto para el efecto y el departamento de contabilidad de la empresa portuguesa contactó al departamento de contabilidad de la empresa francesa. Siguiendo ese contacto se supo que la empresa francesa no había efectuado ningún encargo, que no había recibido ninguna factura y que era falso el correo electrónico del director general, a partir del cual fueron efectuados todos los contactos antes de enviar la mercancía.

La empresa portuguesa interpuso una acción legal contra la aseguradora alegando que la mercancía se perdió durante el transporte y, como tal, el siniestro está incluído en el ámbito de la cobertura de la póliza. La aseguradora contestó alegando que estamos ante un riesgo (fraude informático) que no está previsto en el póliza.

Se trata de un caso concreto que está pendiente en nuestro Bufete a espera de una sentencia del Tribunal.

b. Seguro multiriesgos

En muchas empresas los equipos instalados pueden ser controlados a distancia con recurso a medios informáticos, pudiendo ser dadas instrucciones, para el efecto, a partir de un teléfono móvil. Del conjunto de esos equipos pueden hacer parte la alarma, las maquinas, los ordenadores, el sistema de aire acondicionado, el sistema de iluminación, entre otros.

Un ataque informático podrá desactivar el sistema de alarma y permitir el robo de bienes existentes en la empresa. El riesgo de robo esta incluido en un seguro multiriesgos pero el hecho de tener, en su origen, un ataque informático que no está ni expresamente incluido ni expresamente excluido en el ámbito de la cobertura de la póliza, podrá llevar a la aseguradora a no aceptar pagar la indemnización por los perjuicios causados.

Se trata de un caso concreto que ha ocurrido y que esta en discusión entre aseguradora y asegurado sobre la aceptación (o no) de la responsabilidad por parte de la aseguradora.

7. CONCLUSIONES

1. Los asegurados tienen problemas en saber en concreto lo que pretenden o necesitan y las aseguradoras continúan enfrentándose a grandes dificultades en concretar o prever los riesgos que pueden ocurrir.

2. En lo que respecta a los riesgos cibernéticos no existe un histórico basado en años de experiencia que permita a las aseguradoras prever los riesgos en causa y los siniestros que puedan ocurrir de forma para crear y presentar soluciones equilibradas que satisfagan las necesidades de los clientes.

3. Es importante que existan soluciones standarizadas pero, en determinados casos, el mercado asegurador debe ofrecer soluciones específicas que correspondan a las reales necesidades de los clientes, teniendo por base diligencias precontractuales, incluyendo un análisis riguroso de los riesgos envueltos.

4. Estamos claramente ante una situación especial que puede traducirse en una alta frecuencia aliada a una alta severidad, lo que obliga a las aseguradoras a repensarse sus estrategias de forma a prevenir o disminuir eventuales perdidas substanciales.

5. Los asegurados y aseguradoras luchan contra un enemigo que es invisible y que no puede ser responsabilizado por los daños causados por lo que la posibilidad de ejercicio del derecho de reembolso contra el causador del siniestro es prácticamente inexistente.

6. Los seguros cibernéticos deben incluir coberturas a nivel de los daños propios, que puedan ser básicas o incluir coberturas complementarias, y de responsabilidad civil ante terceros, siendo que las indemnizaciones a pagar puedan alcanzar valores substancialmente altos.

7. Las exposiciones no afirmativas (riesgos silenciosos) constituían una preocupación real para las aseguradoras en el contexto de la acumulación de riesgos en cuanto están en causa seguros en que los riesgos cibernéticos no están expresamente incluidos ni excluidos en el ámbito de cobertura de las respectivas pólizas.

8. La resolución del problema puede pasar por la revisión o actualización de las cláusulas de las pólizas de seguro de forma a excluir expresamente los riesgos cibernéticos o, en alternativa, a incluirlos de forma clara e inequívoca con acuerdo con los asegurados y el consecuente aumento de la prima del seguro.

9. La alternativa pasa por la resolución de los potenciales litígios del Tribunal en el sentido de saber si un determinado siniestro está (o no) incluido en el ámbito de cobertura de la póliza.

BIBLIOGRAFÍA

1.”Undestanding Cyber Insurance – A Structured Dialogue with Insurance Companies”, EIOPA, Publications Office of the European Union, 2018

2. Issues Paper on Cyber Risk to Insurance Sector, IAIS, August 2016.

3. http://blog.mosa.co.za/blog/risk-analysis-and-evaluation-unpacked.

4. Cyber Insurance as Risk Mitigation Strategy – Geneve Association (2018).