ISSN 0123-1154

LOS SEGUROS DE 'CYBER RISK' (A PROPÓSITO DEL CIBERATAQUE MUNDIAL DE FECHA 12 DE MAYO DE 2017)*

CYBER RISK INSURANCE LAW (NEW DEVELOPMENTS UPON MAY 12, 2017 GLOBAL CYBER-ATTACK)

WALDO SOBRINO**

Fecha de recepción: 1 de junio de 2017
Fecha de aceptación: 15 de agosto de 2017
Disponible en línea: 30 de noviembre de 2017

Para Citar este artículo/To cite this article

Sobrino, Waldo, *Los seguros de 'cyber risk'. (A propósito del ciberataque mundial de fecha 12 de mayo de 2017),* 47 Rev.Ibero-Latinoam.Seguros, 137-164 (2017). https://doi.org/10.11144/Javeriana.ris47.lscr

doi:10.11144/Javeriana.ris47.lscr

* Artículo de reflexión realizado a raíz del ciberataque del pasado 12 de mayo.

** Abogado. Doctor en Derecho, Profesor Adjunto de la Facultad de Derecho de la Universidad de Buenos Aires. Contacto: waldo.sobrino@wsya.com.ar

RESUMEN

Con fecha 12 de mayo de 2017 se produjo uno de los más trascendentes ataques globales, donde diferentes hackers produjeron daños a los sistemas de varias empresas en el mundo. Dicho ataque nos brindó una pequeña muestra de lo que puede suceder en el futuro, y –además- también demostró la vulnerabilidad de las empresas. Y una de las enseñanzas que aportó la agresión cibernética, es la demostración que absolutamente todas las empresas se encuentran expuestas a ese riesgo cibernético. Los daños pueden ser desde la generación de 'responsabilidad civil' de la empresa por la divulgación de información confidencial propia o ajena, hasta daños 'patrimoniales' derivados de los daños al sistema de computación, o –aún mayor- en los casos en que se produzca una 'interrupción del negocio' ('Business Interruption'). En la actualidad ya existen Seguros de 'Cyber Risk' en Latinoamérica, donde se puede brindar cobertura para los riesgos de 'Property' y 'Liability', pero debe resaltarse que existen en el mundo una gran variedad de textos de cobertura del seguro, donde es fundamental analizar los alcances de los riesgos cubiertos y las exclusiones de cobertura.

Palabras clave: Seguros; cyber risk; nuevos riesgos; ciberataque; nuevas coberturas de seguros; property; liability; cyber risk; wordings.

ABSTRACT

In May of 2017, servers around the globe were the object of cyberattacks. This was a glimpse of what might happen in the future and showed how vulnerable firms can be. Cyberattacks also showed that firms around the world are subject to running this risk. Damage could entail civil liability resulting from disclosing proprietary information or from damage to property (hardware) or damage resulting from business interruption. Currently there are cyber risks insurance policies available in Latin America where Property and Liability events can be covered; it must be noted that in the world, there are many insurance coverage types of wording, where examining the scope of covered risks and exclusions is paramount.

Keywords: Insurance; cyber risk; new risks; cyberattack; insurance new coverages; property; liability; wording.

SUMARIO

INTRODUCCIÓN. 1. EL CIBERATAQUE MUNDIAL DE FECHA 12 DE MAYO DE 2017. 2. EL *TSUNAMI TECNOLÓGICO* Y LA EVOLUCIÓN DE LA TECNOLOGÍA MODERNA. 3. LOS *NUEVOS RIESGOS* EMPRESARIALES. 4. RIESGO DE *PROPERTY* (DAÑOS PATRIMONIALES). 5. RIESGO DE *LIABILITY* (RESPONSABILIDAD CIVIL). 6. EL SEGURO DE *CYBER RISK*. 6.1. Cobertura de *Property (Daños Patrimoniales)*. 6.2. Cobertura de *Liability (Responsabilidad Civil)*. CONCLUSIONES

INTRODUCCIÓN

1. La temática de los *riesgos cibernéticos* y las consecuencias que puedan producir en las empresas, es una cuestión que nos interesa y preocupa desde hacer varios años.

Así, en el año 2003 publicamos el Libro ***Internet y Alta Tecnología en el Derecho de Daños***[1], donde volcamos los estudios que realizamos en el carácter de alumnos y a la vez también como Profesores de la *Carrera de Especialización* de *Derecho de Alta Tecnología,* que con gran visión de futuro, uno de los precursores en esta temática, como es el gran doctrinario y profesor Horacio Granero[2], comenzó hace alrededor de veinte años en la Universidad Católica Argentina.

2. En aquella época, de análisis preliminares de esta *nueva era*, se pensaba que la cuestión de la *alta tecnología* y los *riegos cibernéticos*, estaban circunscriptas casi para las actividades directamente relacionadas con dichas cuestiones técnicas.

Así se estudiaban las empresas de *Internet Service Providers; Hosting Service Providers* y *Access Internet Providers,* y en especial, se analizaban los casos donde se podía producir la difamación de una persona a través de una página web y las diversas responsabilidades legales que surgían[3].

1. EL CIBERATAQUE MUNDIAL DE FECHA 12 DE MAYO DE 2017

1.1. Recientemente, con fecha 12 de Mayo de 2017 el mundo (especialmente, en el ámbito *empresarial)*, se vió impactado como consecuencia de un *ciberataque* que se produjo a nivel global[4].

---

1 Sobrino, Waldo; *Internet y Alta Tecnología en el Derecho de Daños,* Capítulo I *"Las Nuevas Responsabilidades Legales derivadas de Internet y E-Commerce y los actuales desafíos para el Seguro",* página 17 y siguientes, Editorial Universidad, Buenos Aires, 2003.

2 Granero, Horacio; *"Cómo prevenir un ataque de ransomware (leyendo el Art. 1.757 del Código Civil y Comercial)",* publicado en 'El Dial', Cita: DC2321, de fecha 16 de Mayo de 2017.

3 Sobrino, Waldo; Ponencia *"Nuevas Responsabilidades Legales derivadas de Internet ('Information Providers'; 'Internet Service Providers'; 'Hosting Service Providers' y 'Access Internet Providers') con especial referencia a los casos de difamación de terceros"*, presentada en el *"EcomDer2000" ("Primer Congreso Internacional por Internet sobre Aspectos Jurídicos del Comercio Electrónico")*, organizado por la Facultad de Derecho, de la Universidad de Buenos Aires, en el año 2000.

4 Diario *'Clarín' "Un Ciberataque Global afectó con un virus los sistemas informáticos de 74 países"*, página 1, de fecha 13 de Mayo de 2017.

Así, en un principio se señalaba que los hackers habían producido alrededor de 80.000 incidentes, que afectaron a personas físicas y jurídicas de más de setenta (70) países.

Con posterioridad, al día siguiente, los medios determinaron que en realidad se habían producido 130.000 ataques y que los mismos habían ocurrido en cien (100) países[5].

Las consecuencias fueron avanzando y con fecha 15 de Mayo de 2017, se explicaba que se habían producido más de 200.000 incidentes en computadoras de más de ciento cincuenta (150) países[6].

1.2. De esta manera, en forma casi indiscriminada, se realizaron ataques tanto en domicilio particulares, como asimismo en empresas comerciales, como la francesa Renault (que tuvo que detener su producción) y la norteamericana Fed Ex y también en entidades públicas como el Banco Central de Rusia, el sistema de salud de Inglaterra, los trenes de Alemania, Universidades de Italia, etc.

Más allá que algunos expertos hablan de un *"ciber-apocalipsis"*, es que entendemos que esta dura experiencia debe servir de alerta y de llamado de atención.

Por ello, es que este incidente global no solo debe implicar un disparador para actualizar y mejorar los sistemas de seguridad (v.gr. *firewall, back ups*, etc.) contra los hackers, sino también debe servir para merituar las consecuencias que en el futuro este tipo de ataques puede producir en instituciones públicas y empresas privadas (y la trascendencia fundamental que tiene la contratación de un Seguro de *Cyber Risk)*[7].

1.3. Es pertinente recordar que en el año 2016, las Compañías de Seguros suscribieron seguros de *cyber risk* por un monto de Mil tres-

5 Diario *'Clarín' "El Ciberataque ya afecta a más de 100 países y es de un nivel 'sin precedentes'"*, página 30, de fecha 14 de Mayo de 2017.

6 Diario *'Clarín' "La policía de la Unión Europea advierte que el ciberataque podría repetirse hoy"*, página 26, de fecha 15 de Mayo de 2017.

7 Ver: *"Firms hit by Cyber attack could face lawsuits over lax security: Legal Experts"*, publicado en *'Insurance Journal'*, de fecha 16 de Mayo de 2017.

cientos millones de dólares (U$S 1.300.000.000), calculándose que para el año 2022, aumentará más de diez veces, llegándose a una suscripción de U$S 14.000.000.000[8].

1.4. Respecto a las consecuencias del *ciberataque global* en los seguros de *cyber risk*, hay que señalar que no hubo pérdidas muy significativas, dado que si bien en los Estados Unidos muchas empresas tienen contratado este seguro[9], la realidad es que la gran mayoría de los ataques se produjeron en empresas radicadas en Europa y Asia donde la contratación del seguro de *cyber risk* es sustancialmente menor[10].

2. EL *TSUNAMI TECNOLÓGICO* Y LA EVOLUCIÓN DE LA TECNOLOGÍA MODERNA

2.1. La sociedad moderna evoluciona de una manera tan rápida que a todos en general nos cuesta llegar a comprender cabalmente, y –en particular– a los hombres de derecho nos obliga a pensar de manera diferente.

Así, este *nuevo pensamiento disruptivo* nos embarca en la apasionante tarea de intentar estudiar situaciones y cuestiones que no tienen antecedentes.

2.2. Mas, señalamos que estos grandes cambios no necesitan mucho tiempo para su desarrollo. Para ello basta analizar la situación de la tecnología hace solo diez o veinte años atrás.

Parecería que estamos hablando –tecnológicamente– casi de la *Era Paleolítica.*

2.3. Y, este verdadero *tsunami tecnológico* tiene consecuencias puntuales y específicas no solo en la vida diaria de nuestra sociedad, sino

8 Ver: *"Fitch prevé un aumento de la demanda de ciberseguros tras los ataques recientes de ransomware"*, publicado en Inese.es, de fecha 17 de Mayo de 2017.

9 Middleton, Kirsty And Kazamia, María; *"Cyber Insurance: Underwritting, Scope of cover, Benefits and Concerns"*, en *The 'Dematerialized' Insurance*, bajo la Dirección de Pierpaolo Marano, Ioannis Rokas y Peter Kochenburger, Parte III, páginas 185 y siguientes, Editorial Springer, Suiza, 2016.

10 Ver: *"El ataque de Ransomware global golpea a los Aseguradores cibernéticos, pero las pérdidas son limitadas"*, publicado en Inese.es (tomando como fuente *Business Insurance)*, de fecha 16 de Mayo de 2017.

también en los diversos aspectos de los *riesgos y las responsabilidades legales.*

Para analizar estos *nuevos mundos tecnológicos* van a resultar indispensables las mentes frescas y abiertas de los jóvenes doctrinarios, como por ejemplo el profundo estudioso **Sebastián Cerda**[11], que incursionan en estas áreas con gran conocimiento.

3. LOS *NUEVOS RIESGOS* EMPRESARIALES

3.1. Si bien en Latinoamérica en general y en Argentina en particular, no se le había dado la trascendencia que corresponde a esta *nueva era tecnológica,* respecto a los *riesgos empresariales*, es importante señalar que en las sociedades desarrolladas, como Estados Unidos, la mayoría de los países Europa[12] y Japón[13] ya se estaban ocupando proactivamente del tema[14].

A guisa de sencillo ejemplo, podemos recordar la profética nota de **Hilary Tuttle**[15] en la *Revista 'Risk Management'* donde bajo el título ***"The 2017 Cyberrisk Landscape"*** menciona la problemática –por ejemplo– del *'Ransomware'*, es decir, la *extorsión* que se produce por una especie de *secuestro virtual* de los archivos de las computadoras, que son *encriptados* y luego son *liberados,* por medio del pago de una suma de dinero.

11 Cerda, Sebastián; Ponencia *"La exposición de la empresas argentinas a los riesgos Cibernéticos y la falta de cobertura a los mismos en Argentina"*, presentada en el *XVI Congreso Nacional de Derecho de Seguros***,** organizado por la Asociación Internacional de Derecho de Seguros (A.I.D.A.), Rama Argentina, en la Ciudad de La Plata, Argentina, en el mes de Septiembre de 2016.

12 *"Ciberseguros: la transferencia del ciberriesgo en España"*, publicado por Thiber, Capítulo 3 *"Los Ciberseguros"*, Madrid, España, Abril de 2016.

13 Koezuka, Tadao; *"The Cyber Insurance in Japan", en The 'Dematerialized' Insurance*, bajo la Dirección de Pierpaolo Marano, Ioannis Rokas y Peter Kochenburger, Parte III, páginas 201 y siguientes, Editorial Springer, Suiza, 2016.

14 Ver: *"El Riesgo Cibernético es un desafío cada vez mayor para todas las Industrias"*, donde se informa que expertos internacionales se encuentran trabajando en el *"Proyecto de Seguros entre la Unión Europea y Estados Unidos (EU - U.S. Insurance Project)"***,** publicado en *"Buena Fuente"*, de fecha 23 de Enero de 2017.

15 Tuttle, Hilary; *"The 2017 Cyberrisk Landscape"*, página 4, publicado en la Revista *"Risk Management"*, donde se mencionan –entre otros riesgos– *Ransonware; IoT Anarchy (Internet of Things);* etc., página 16, Volume 64, Issue 1, New York, de fecha Enero / Febrero de 2017.

Justamente, ello es lo que aconteció con fecha 12 de Mayo de 2017[16], cuando se produjo a nivel global, lo que se denominó uno de los mayores ciberataques mundiales

3.2. De manera liminar, se puede señalar que los *riesgos cibernéticos* de las empresas[17], se pueden estudiar dentro de las pautas de *Liability (Responsabilidad Civil)*[18-19] y también del riesgo de *Property (Daños Patrimoniales)*[20].

3.3. Así, corresponde tener presente un Informe del año 2017, efectuado por Allianz[21], que es una de las empresas de reaseguros más destacadas a nivel internacional, donde se señala que el *riesgo cibernético* se encuentra en tercer lugar, dentro de las preocupaciones de las empresas

Incluso, se debe señalar otro Informe del año 2017, que habla de una *"Tormenta Perfecta"* para las empresas europeas, vinculadas con el riesgo de *Cyber Risk*, destacando el tema de las empresas de infraestructura, como pueden ser los proveedores de agua, centrales nucleares, de energía, etc.[22], lo que lleva a varios autores a hablar de un hipotético *"Cyber Pearl Harbor"*[23].

16 Ver: Diario *Clarin "Un Ciberataque Global afectó con un virus los sistemas informáticos de 74 países"*, página 1, de fecha 13 de Mayo de 2017.

17 Anderson, Eugene - Stanzler, Jordan - Masters, Lorelie; *Insurance Coverage Litigation*, Chapter 18 *'Coverage for Cyberspace and Computer Liability',* parágrafo n° 18.04 *'Coverage of High-Tech Claims under Traditional Insurance',* acápite (I) *"Electronic Funds Transfer (EFT) Insurance",* página 18-41, Editorial Wolters Kluwer Law and Business, 2nd edition, New York, 2015.

18 Ver: *"Allianz Risk Barometer 2017 - Top Risks in focus: Cyber incidents"*, en www.agcs.allianz.com / insights / expert-risk-articles / allianz-risk-barometer-2017-top-risks- cyber-incidents

19 Sobrino, Waldo - Gava, Adriel - Tortorelli, Mercedes (Directores); *Ley de Seguros Comentada*, Art. 109*,* publicada en www.laleyonline.com.ar

20 Murlick, Brad - Gold, Joshua; *"Securing coverage for Cyberattacks"*, página 18, publicado en *'Risk Management'*, del mes de Octubre de 2016.

21 Ver: *"Allianz Risk Barometer 2017 - Top Risks in focus: Cyber incidents"*, en www.agcs.allianz.com / insights / expert-risk-articles / allianz-risk-barometer-2017-top-risks-cyber-incidents

22 Risi, Walter - Almada, Pablo; *"Prepararse para Ciberataques a Infraestructuras"*, donde se señala: *"...la pregunta que se impone es: ¿ los países y las empresas están preparadas para prevenir y soportar un ataque informático ?..."*,
Agregando luego: *"...¿ Un posible ciberataque a áreas de infraestructura crítica como lo son el sistema energético, las telecomunicaciones, o el control del transporte aéreo, qué impacto pueden tener en un país y en las empresas concesionarias o responsables de prestar servicios básicos a la comunidad ?...",* publicado en el Diario 'El Cronista', página 14, de fecha 1° de Febrero de 2017.

23 Ver: *"Europe's Firms face potential 'Perfect Storm' of Cyber Threats: Marsh Mc Lennan Report"*, publicado en *"Insurance Journal"* de fecha 27 de Enero de 2017.

Todo ello señala que el análisis del *Cyber Risk* ya no se debe estudiar como algo excepcional, sino que nos demuestra que hoy en día se trata de un riesgo generalizado para muchas empresas[24].

Asimismo, también se debe tener presente que existen muchas cuestiones que todavía no tienen una normativa específica, como los *Bitcoins*[25] que es una especie de *nueva moneda* (que se la utiliza para cobrar las *extorsiones* de los *ransomware)*; la aparición de nuevas cuestiones como *Blockchain*[26], etc.

3.4. Tanta trascendencia tiene el riesgo de *cyber risk* que **Mary Jo White**, en su carácter de Jefe de la *Securities and Exchange Commission (S.E.C.)* señaló en forma puntual y específica que *"…los ataques cibernéticos representan el mayor riesgo sistémico en los Estados Unidos…"*[27].

4. RIESGO DE *PROPERTY* (DAÑOS PATRIMONIALES)

4.1. La extensión de los *riesgos* vinculados con *daños patrimoniales* no solo deben analizarse para las empresas comerciales, sino también que pueden tener consecuencias en las personas particulares.

4.2. Un sencillo ejemplo de ello, es el vinculado con la *'Internet of Things' ('IoT')*[28], es decir, todos los aparatos electrónicos que se tienen en los *hogares*, que se pueden controlar desde un celular o la *tablet,* como pueden ser no solo los aires acondicionados, los televisores, sino –de manera fundamental– las *cámaras de seguridad*, las *alarmas contra robos*, etc.[29].

---

24 *"Ciberseguros: la transferencia del ciberriesgo en España"*, publicado por Thiber, Capítulo 3 *"Los Ciberseguros"*, acápite .3.4.2) *"Exclusiones Principales"*, donde se resaltan *"…los riesgos asociados a las infraestructuras críticas y sobre todo, los sistemas de control industrial..."*, recordando que *"…determinadas industrias, como la energética…tienen altamente automatizado la generación y distribución de energía o la producción…",* página 27, Madrid, España, Abril de 2016.

25 Palley, Stephen; *"Bitcoin, Blockchain and Insurance: New Tech, Old Rules"*, publicado en Anderson Kill *"Policyholder Advisor"*, de fecha Mayo / Junio de 2016.

26 Crawford, Mark; *"The Insurance implications of Blockchain"*, publicado en la *Revista 'Risk Management',* Volume 64, Issue 2, página 25, del mes de marzo de 2017.

27 Joost, Eric; *"Cyber Risk: un riesgo como ningún otro"*, publicación de *Willis Towers Watson*, de fecha 29 de Septiembre de 2015.

28 Snowdon, Tamara; *"Internet of Things: The Risk Manager perspective"*, publicado en *Beecher Carlson Insurance Services,*, del mes de Diciembre de 2016.

29 Ver: *"Connected Homes heighten need for Personal Cyber Insurance"*, donde se señala que gran parte de los hogares de Estados Unidos, tienen conectados sus sistemas de televisión, aire acondicionado, etc. a través de internet y que en varias oportunidades *hackers* han irrumpido, dañando dichos aparatos.

4.3. Y, en el caso de las *empresas* las consecuencias *patrimoniales* de un *ciberataque* pueden ser sustancialmente más gravosas, dado que se puede llegar a detener la cadena de producción, o se pueden robar secretos comerciales, o destruir archivos de la empresa, etc.

Existen ciertas empresas que realizan *Ventas on line*, o prestan servicios de *Internet Service Providers* o que realicen *Hosting de páginas web*, etc, cuya vinculación de internet es casi excluyente.

Pero, para todo el resto de las empresas, también su *dependencia crítica* de todo el sistema de *software* es casi absoluta, dado que las computadoras son el centro neurálgico de la actividad empresaria[30].

Y, día a día, dicha dependencia se va acentuando cada vez más, como sucede con las empresas que realizan estibajes con depósitos automatizados, o las automotrices, donde se fabrican los automóviles con robots, etc.[31].

Tanta es la importancia del tema, que se debe señalar que con fecha 1° de Mayo de 2017, en la primera página del Diario *"The Wall Street Journal"*, se realiza un minucioso estudio de estas cuestiones, por medio de la nota ***"Hackers found holes in Bank Network"***, donde se exponen distintos ciberataques a diferentes Bancos en varias partes del mundo[32].

4.4. Incluso, en los daños de *Property* vinculados con los *seguros*, es fundamental analizar el *Business Interruption*[33], dado que un ataque

Por ello, ya existen *Seguros de Cyber Risk* para *Hogares*, publicado en *"Insurance Journal"* de fecha 27 de Enero de 2017.

30 Murlick, Brad - Gold, Joshua; *"Securing coverage for Cyberattacks"*, página 18, publicado en *'Risk Management'*, del mes de Octubre de 2016.

31 *"Ciberseguros: la transferencia del ciberriesgo en España"*, publicado por Thiber, Capítulo 3 *"Los Ciberseguros",* página 27, Madrid, España, Abril de 2016.

32 Zabala, Amparo; *"El Ciber Riesgo y Seguro"*, donde se explica que en un principio los seguros cibernéticos estaban enfocados para las empresas *"puntocom"*; posteriormente, se fueron ampliando en forma genérica a las empresas tecnológicas y en la actualidad se tiene a la vista la protección de la mayoría de las empresas, publicado en *"Riesgos Globales y su aseguramiento",* e-Letter N° 19 de *Community of Insurance*, del mes de Octubre de 2015.

33 Gold, Joshua; *"Adjusting Insurance Coverage to meet shifting Cyberattack Risks"*, página 31, donde se expone respecto a los *Cyberattacks* que *"...have important implications for property damage,* ***business interruption****, and corporate reputation...",* publicado en *'Risk Management'*, del mes de Octubre de 2015.

de *hackers*, puede llegar a generar *daños consecuenciales*[34] de gran magnitud[35].

En efecto, dicha *interrupción de negocios* puede tener repercusiones económicas a gran escala por la *pérdida de beneficios,* debiendo analizarse no solo el *Business Interruption* directo, sino también el denominado *Business Interruption Contingente*[36].

Es importante resaltar que este nuevo escenario que estamos analizando, se van a tener que reanalizar atávicos conceptos que se utilizan en el ámbito de los Seguros de *Business Interruption*, como –por ejemplo– es la cuestión de la necesidad indispensable de un *daño físico*[37].

Ello es así, porque a diferencia de los tradicionales seguros de *Business Interruption*[38], en los seguro de *Cyber Risk* válidamente existe cobertura de *interrupción de negocios* aunque *no exista un daño físico*[39].

Volviendo al caso del *ciberataque mundial* de fecha 12 de Mayo de 2017, en aquellos casos donde el *ransomware*[40] hubiera encriptado ciertos

34 Michelbacher, G., *Casualty Insurance Principles*, página 6, donde se hace referencia a los *"consequential losses"*, donde se expone que *"...loss from destruction of, or damage to, property often extends beyond mere physical value of the property directly affected. There may be consequential losses, such as loss of use of the property, or loss of other property due the original loss..."*, produciendo, por ejemplo *loss of profits*. Ed. Mc Graw - Hill Company, Nueva York, 1930.

35 Zola, Jared; *"Swatch fire losses and Contingent Business Interruption Coverage"*, publicado en *Insurance Journal*, de fecha 30 de Diciembre de 2015.

36 Ver: *"Purchasers Guide to Cyber Insurance Products"*, publicación del *"Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security"*, donde se explica *"...while some policies cover contingent business interruption (i.e. a cyber incident at a third party causes a business interruption for the policyholder), the sublimit for such coverage usually is very limited..."*, publicado en el año 2016.

37 Beecher Carlson; **"***Cyber: a Tale of two markets" (Inconsistencies in Cyber insurance policies can lead to 'Swiss cheese towers' of coverage)"*, publicado en *Risk & Insurance* con fecha 15 de de Marzo de 2017.

38 Torpey, Daniel - Lentz, Daniel - Barret, David; *The Business Interruption Book (Coverage, Claims and Recovery)***,** Chapter 1: *"Insuring Changing Exposures"*, página 11, Editorial The National Underwriter Company, Estados Unidos, Ohio, 2004.

39 Freedman, Anne; *"Cyber Business Interruption: attacks on internet infrastructure commence, leaving unknown risks for insureds and insurers alike"*, publicado en *'Riskandinsurance'* de fecha 7 de abril de 2017.

40 Granero, Horacio; *"Cómo prevenir un ataque de ransomware (leyendo el Art. 1.757 del Código Civil y Comercial)"*, publicado en 'El Dial', Cita: DC2321, de fecha 16 de Mayo de 2017.

documentos y/o archivos de la empresa asegurada, ello puede generar una *interrupción de negocios*[41].

Y, más allá de la existencia o no de un típico *daño físico*, es que se trataría de un siniestro amparado por el seguro de *Cyber Risk*, dado que la *causa* de la *pérdida de beneficios*, es una *riesgo* expresamente cubierto por la póliza de seguros[42].

Es por ello, que alerta la doctrina anglosajona, en el sentido que: *"... policyholders should seek Business Interruption insurance that does not tie insurance coverage to some physical act or event..."*[43].

Reiteramos que no estamos hablando de ejemplos hipotéticos, sino de hechos que ya han sucedido, como explica el *"New York Times International Weekly"*, en Febrero de 2017[44], donde analiza la situación bajo el título *"Hackers usan un software para secuestrar datos y pedir rescate"*.

En dicha noticia se relata lo sucedido al Hotel *Romantik Seehotel Jaegerwirt*, donde a través de un *ransomware* se encriptaron los accesos a las habitaciones y al sistema de reservaciones, obligando al hotel a pagar el *rescate* para desbloquear los sistemas[45].

41 Healy, Daniel - Palley, Stephen; *"Internet Down? Insurance may cover your losses after a Denial of Service Attack"*, donde explican *"...some policy forms may cover* ***purely economic loss,*** *without requiring underlying* ***property damage…"***, agregando *"...this can be the case under a variety of cyber insurance policy forms, including network liability coverage that specifically cover DDoS attacks..."*, publicado en Anderson Kill *"Policyholder Advisor & Alert"*, de fecha 25 de Octubre de 2016.

42 Papa, Ronald - Gilinsky, Marshall; *"Business Income Coverage, a critical and often overlooked area of Property Insurance"*, publicado en *'Anderson Kill Policyholder Advisor'*, de fecha Noviembre / Diciembre de 2016.

43 Anderson, Eugene - Stanzler, Jordan - Masters, Lorelie; *Insurance Coverage Litigation*, Chapter 18 *'Coverage for Cyberspace and Computer Liability',* parágrafo n° 18.04 *'Coverage of High-Tech Claims under Traditional Insurance',* acápite (G) *"Business Interruption Insurance",* página 18-39, Editorial Wolters Kluwer Law and Business, 2nd edition, New York, 2015.

44 Ver: *"New York Times International Weekly"*, página 5, publicado en el Diario *'Clarín'*, de fecha 11 de Febrero de 2017.

45 Ver: *"Austrian Hotel faces Ransomware attack"*, publicado en la *Revista 'Risk Management',* Volume 64, Issue 2, página 17, del mes de marzo de 2017.

5. RIESGO DE *LIABILITY* (RESPONSABILIDAD CIVIL)

5.1. Otro de los grandes riesgos que tienen las empresas frente al ataque de un *hacker*, está referido a la *responsabilidad civil*[46] que se puede generar por los daños producidos a terceros o a los propios clientes[47].

5.2. En una primera época, se puso énfasis en las empresas estrechamente relacionadas con la actividad de internet (v.gr. *Internet Service Providers; E-Commerce;* etc.)[48].

Así, si se produce un *D.o.S. (Denied of Service)* de una empresa que provee la conexión a internet a una empresa de venta *on line* como consecuencia de un ataque de un *hacker*, es que se pueden ocasionar pérdidas millonarias, con las consiguientes responsabilidades legales[49].

5.3. Y, en la actualidad dichas responsabilidades legales se han generalizado[50].

Ello es así, ya que existen innumerables alternativas de responsabilidad civil, como podría ser el caso que un *hacker* invada los archivos de un Banco y saque a la luz los datos confidenciales de los clientes; o que se expongan en internet las Historias Clínicas de un Hospital; etc.[51].

---

46 Sobrino, Waldo - Gava, Adriel - Tortorelli, Mercedes (Directores); *Ley de Seguros Comentada*, Art. 109*,* publicada en www.laleyonline.com.ar

47 Sobrino, Waldo; Ponencia *"El Seguro de responsabilidad Civil frente al desafío de las nuevas Tecnologías (especialmente referido a Internet & E-Commerce)",* presentado en las *"Jornadas Nacionales de Seguros 'Córdoba 2000'" y "VII Conferencia Internacional de Seguros"*, en la Ciudad de Villa Carlos Paz, Córdoba. realizada los días 21, 22 y 23 de Septiembre de 2000.

48 Sobrino, Waldo; *Internet y Alta Tecnología en el Derecho de Daños*, Capítulo I *"Las Nuevas Responsabilidades Legales derivadas de Internet y E-Commerce y los actuales desafíos para el Seguro",* página 17 y siguientes, Editorial Universidad, Buenos Aires, 2003.

49 Ver: *"Firms hit by Cyber attack could face lawsuits over lax security: Legal Experts"*, publicado en *'Insurance Journal'*, de fecha 16 de Mayo de 2017.

50 Cerda, Sebastián; Ponencia *"La exposición de la empresas argentinas a los riesgos Cibernéticos y la falta de cobertura a los mismos en Argentina"*, presentada en el *XVI Congreso Nacional de Derecho de Seguros***,** organizado por la Asociación Internacional de Derecho de Seguros (A.I.D.A.), Rama Argentina, en la Ciudad de La Plata, Argentina, en el mes de Septiembre de 2016.

51 Ver: *"Allianz Risk Barometer 2017 - Top Risks in focus: Cyber incidents"*, en www.agcs.allianz.com / insights / expert-risk-articles / allianz-risk-barometer-2017-top-risks-cyber-incidents

También es pertinente señalar que puede surgir la responsabilidad civil de una empresa, por la transmisión de virus, la violación de derechos de propiedad intelectual, o por calumnias, difamaciones, etc.[52].

6. EL SEGURO DE *CYBER RISK*

A nivel mundial la cobertura de los *riesgos cibernéticos* es bastante reciente y en Latinoamérica (y en Argentina, en particular), recién se está comenzando a desarrollar

Entre otras cuestiones, ello significa que no existen *textos uniformes*[53] o *pólizas standards*[54], sino que las coberturas, condiciones, cláusulas y exclusiones de cobertura[55], van a depender específicamente del *wording* que se aplique[56].

Incluso, atento la gran variedad de textos[57], es que algunos autores señalan que por el momento es muy difícil hablar técnicamente de un Seguro general de *Cyber Risk*[58].

Dicha dispersión de cláusulas y condiciones, no solo va a generar que se deben extremar las precauciones a la hora de contratar los segu-

52 Raptis, Steve; *"Analyzing Cyber Risks Coverage"*, publicado en *"Risk and Insurance"*, de fecha 13 de Marzo de 2015.

53 Harrington, Joseph; *"Cyber Insurance: many choices now that there is not choice"*, donde citando a Stephanie Snyder, señala que *"…Cyber insurance is available from about 70 carriers, most of them with very different coverage features…"* publicado en *'Insurance Journal'*, de fecha 12 de Abril de 2017.

54 Koezuka, Tadao; *"The Cyber Insurance in Japan"*, en *The 'Dematerialized' Insurance*, bajo la Dirección de Pierpaolo Marano, Ioannis Rokas y Peter Kochenburger, Parte III, páginas 201 y siguientes, Editorial Springer, Suiza, 2016.

55 Gold, Joshua - Malone, Cort; *"Data Security: Tips and Red Flags when buying Cyber Insurance"*, donde se analiza la *Exclusión de cobertura* referida a *"Violation of Statute, Rule, Law or Consumer Protection Law",* donde se expone que *"…it is not uncommon for regulators and others to assert that the policyholder's data handling and conduct violated state or federal law…",* publicado en *"Enforce"*, de fecha 1° de Septiembre de 2013.

56 Entre otras, pueden mencionarse los *wordings* de A.I.G *'Cyber Edge'*; HISCOX *'Cyber and Data';* Travelers, Chubb; etc.

57 Raptis, Steve; *"Analyzing Cyber Risks Coverage"*, publicado en *"Risk and Insurance"*, donde señala que existen alrededor de cincuenta (50) Compañías de Seguros que comercializan *Cyber Insurance,* de fecha 13 de Marzo de 2015.

58 Chesler, Robert; *"Cyber Insurance Coverage: the next wave?"*, donde expone *"…to speak of 'cyber insurance' is a misnomer. No standard policy form exists and different policies can differ dramatically…",* publicado en *"New Jersey Alert"*, de fecha 9 de Marzo de 2015.

ros de *cyber risk*[59], sino que –además– van a implicar una complicación adicional cuando se deban liquidar los siniestros[60] en esta temática tan particular y novedosa[61].

Por ello, debemos recordar también la evolución que sufrieron los Seguros de *Directores & Officers*, donde en sus primeras épocas, existían gran diversidad de *wordings*, que llevó a la Jurisprudencia de Estados Unidos (***"Keating vs. National Union Fire Insurance Company"***[62] y a la doctrina a afirmar que era una verdadera ***"Torre de Babel"***[63].

Así, en el caso de los *Cyber Insurances* sucede algo análogo, dado que esta gran variedad de textos[64], lleva a la doctrina (por todos: **Robert Chesler**)[65] a afirmar que nos encontramos en el *salvaje oeste ('wild west')*, dado que cada Aseguradora ofrece el *wording* que le parece más conveniente.

Como consecuencia de ello, es que como bien explica la moderna doctrina de nuestro país (por ejemplo el estudioso autor **Sebastián Cerda)**[66], las empresas deberán analizar el profundidad del *wording* que

59 Middleton, Kirsty and Kazamia, María; *"Cyber Insurance: Underwritting, Scope of cover, Benefits and Concerns"*, en *The 'Dematerialized' Insurance*, bajo la Dirección de Pierpaolo Marano, Ioannis Rokas y Peter Kochenburger, Parte III, páginas 185 y siguientes, Editorial Springer, Suiza, 2016.

60 Sobrino, Waldo; *"El Proceso de Liquidación de Siniestros de Seguros y 'El Proceso' de Franz Kafka: ¿ dos almas gemelas ?"*, publicado en el Diario 'La Ley', de fecha 13 de Octubre de 2009.

61 Mandel, Christopher; *"The Claims Function and Best Practices",* donde se explican las mejores prácticas para la Liquidación de Siniestros y se resalta que *"...some types of claims we're now seeing are somewhat different in areas as those related to Cyber-Policies..."*, publicado en *'IRMI - Expert Commentary'*, de fecha Marzo de 2017.

62 Ver: *The Directors & Officers Book (a comparison guide to Directors & Officers Liability Insurance Policies)*, página 4, Ed. Griffin Communications Inc, California, Estados Unidos, 2001.

63 Ver: *RiskVue Plus***;** *"Demand Careful Policy review"*, donde se afirma que *"...one judge reviewing a Directors and Officers liability policy compared the policy wording to a linguistic Tower of Babel..."*, de fecha 4 de Enero de 2007.

64 Harrington, Joseph; *"Cyber Insurance: many choices now that there is not choice"*, publicado en *'Insurance Journal'*, de fecha 12 de Abril de 2017.

65 Chesler, Robert; *"Federal Trade Comission vs. Wyndham Worldwide Corp Decision highlights need for robust Cyber-Insurance Policies"*, donde explica que los asegurados *"...should be forewarned that the cyber insurance market is like the Wild West...",* publicado en *Anderson Kill Policyholder,* del mes de Septiembre de 2015.

66 Cerda, Sebastián; Ponencia *"La exposición de la empresas argentinas a los riesgos Cibernéticos y la falta de cobertura a los mismos en Argentina"*, presentada en el *XVI Congreso Nacional de Derecho de Seguros***,** organizado por la Asociación Internacional de Derecho de Seguros (A.I.D.A.), Rama Argentina, en la Ciudad de La Plata, Argentina, en el mes de Septiembre de 2016.

se les ofrece[67], para determinar si satisface las necesidades de cobertura del riesgo que desean amparar[68].

Complementando y profundizando lo antes expuesto, es que debemos resaltar que de acuerdo a la normativa aplicable, la Compañía de Seguros y el Productor de Seguros tienen que cumplir puntual y específicamente (y más aún en el seguro de *Cyber Risk)*, con el *Deber de Información*, el *Deber de Consejo* y el *Deber de Advertencia*[69].

Todo ello, bajo apercibimiento de aplicar las sanciones previstas en la legislación vigente y lo señalado por la doctrina[70], en el caso que no se satisfagan las *expectativas razonables*[71] del asegurado[72].

Allí del brillante doctrinario explica que dentro de la gran cantidad de *riesgos* que existen en la *Tecnología de la Información y Comunicación (T.I.C.)*, entre otros pueden mencionarse "*…la manipulación de datos confidenciales; hackeo de servidores; robo y/o divulgación no autorizada de datos; virus; piratería; espionaje, sabotaje, guerra; afectación de infraestructuras de internet; spam; denegación de servicios; robo, suplantación y/o revelación de identidades, fraudes y criminalidad informática; extorsión; malware*; *entre otros…".*

67 Chesler, Robert – Yousef, Christina; *"Six Insurance Coverage Lessons from 2016"*, donde bajo el título *"Customize your Cyber Policy"* comentan la Sentencia *"P. F. Chang's vs. Federal Insurance Company",* de fecha 26 de Mayo de 2016, donde se rechazó el reclamo del asegurado, porque el seguro no se ceñía a sus necesidades y por tanto el siniestro denunciado no tenía cobertura, publicado en Anderson Kill *"Policyholder Advisor"*, Volumen 26, Número 1, de fecha Enero / Febrero de 2017.

68 Gold, Joshua - Halprin, Peter; *"Cyber Insurance Disputes: will Arbitration Clauses be a battleground?"*, publicado en *'Policyholder Advisor'*, Volume 25, Issue 2 Marzo/Abril de 2016.

69 Sobrino, Waldo; *Seguros y el Código Civil y Comercial (y su relación con la Responsabilidad Civil, el Derecho del Consumo, la Constitución Nacional y los Tratados Internacionales)*, Capítulo .IX.1) *"El 'Deber de Información: y su relación con el 'Deber de Prevención', el 'Deber de Precaución', el 'Deber de Consejo' y el 'Deber de Advertencia'"***,** páginas 445 a 488, Editorial La Ley, Julio de 2016.

70 Sobrino, Waldo; *"El 'Deber de Información', de 'Consejo' y de 'Advertencia' en materia de Seguros"*, en especial, Capítulo VIII *"El Deber de Consejo",* publicado en el Diario 'La Ley', página 2, de fecha 1° de Febrero de 2017.

71 Donnelly, Thomas - Brown, Craig; *Insurance Contract Interpretation*, Chapter 9 *"Circumvention of Policy Language"*, acápite 5 *"Reasonable Expectations",* (b) *Reasonable Expectations in the United States,* página 177, Nota 69, donde se cita la Sentencia *"Brissette vs. Westbury Life Insurance Company"* , donde se establece *"…generally, the aim of that doctrine is to make certain that insurance policies provide the coverage which the insured can reasonably expect to receive…",* Ed. Carswell - Thomson Reuters, Canada, 2014.

72 Anderson, Eugene - Stanzler, Jordan - Masters, Lorelie; *Insurance Coverage Litigation*, Capítulo 2 *"Rules of Insurance Policy Interpretation"*, acápite 2.01 (B), donde con relación a la doctrina de las *"Expectativas Razonables"* se señala que *"…In 1970, Professor Keeton formulated that doctrine as follows: 'the objectively reasonable expectations of applicants and intended beneficiaries regarding the terms of insurance contracts will be honored even though painstacking study of the policy provisions would have negated those expectations'...",* página 2-19, Editorial Wolters Kluwer Law and Business, 2nd edition, New York, 2015.

Asimismo, las *empresas aseguradas*, en especial las *grandes empresas* deberán analizar en profundidad las Cláusulas y Condiciones del Seguro de *Cyber Risk*, en especial las *Caducidades*[73]. y las *Exclusiones de cobertura*[74], para determinar si se les están brindando las coberturas que necesitan[75] para amparar sus riesgos empresariales[76].

Complementando lo recién expuesto, es que brevemente haremos algunos comentarios de los Seguros de *Cyber Risk*[77], en particular en las coberturas de *Daños Patrimoniales (Property)* y *Responsabilidad Civil (Liability)*[78].

6.1. Cobertura de *Property (Daños Patrimoniales)*

6.1.1. Coberturas de *Daños Patrimomiales (Property)* en el Seguro de *Cyber Risk:*

Entre algunas de las coberturas del Seguro de *Property* podemos mencionar las siguientes:

---

73 Sobrino, Waldo; *"Exclusiones vs. Caducidades: las (pseudo) Exclusiones de cobertura y las Caducidades del seguro (una sutil manera de restringir el poder de los jueces, a través de una ilegal estrategia burocrática)"*, publicado en *'Revista de Responsabilidad Civil y Seguro'*, del mes de Febrero de 2013.

74 Raptis, Steve; *"Analyzing Cyber Risks Coverage"*, donde bajo el título de *"Exclusions for acts of Terrorism or war"* expone que *"…its unclear to what extent insurers rely on these exclusions when data breach result from an organized attack by a foreign nation or hostile organization…",* publicado en *"Risk and Insurance"*, de fecha 13 de Marzo de 2015.

75 *"Ciberseguros: la transferencia del ciberriesgo en España"*, publicado por Thiber, Capítulo 3 *"Los Ciberseguros"*, acápite .3.4.2) *"Exclusiones Principales"*, donde dentro de las *exclusiones de cobertura,* se señala: *"…Guerra y Terrorismo, a pesar que a día de hoy existen coberturas afirmativas (o expresas) relacionadas con ataques ciberterroristas…",* página 27, Madrid, España, Abril de 2016.

76 Gold, Joshua; *"Beware of Holes in your Cyber Insurance Policies"*, publicado en *"Policyholder Advisor & Alert"*, de fecha 14 de Mayo de 2015.

77 Chesler, Robert; *"Cyber Insurance Coverage: the next wave?"*, donde explica *"…nine categories of cyber insurance currently exist, and each company must decide which components it needs. The key coverages includes:*
1) coverage against privacy lawsuit by individuals
2) coverage against govermental privacy investigation
3) cyber-business interruption coverage
4) cyber-extortion
5) media coverage, such as defamation, trademark and copyright
6) network disruption
7) crisis response costs
8) network loss or damage; and
9) electronic theft…", publicado en *"New Jersey Alert"*, de fecha 9 de Marzo de 2015.

78 Sobrino, Waldo - Gava, Adriel - Tortorelli, Mercedes (Directores); *Ley de Seguros Comentada*, Art. 109*,* publicada en www.laleyonline.com.ar

 # Robo de Datos o de dinero

 # Destrucción o contaminación de Datos o Información

 # Costos de expertos para descubrir las causas de los daños o hackeo

 # Extorsión

 # Denegación de Acceso

 # Business Interruption

etc.

a) ***Robo de Datos o de dinero:***

Se ampara el *robo de datos* o el *robo de dinero* que sufra la empresa asegurada[79].

b) ***Destrucción o contaminación de Datos o Información:***

Se cubren los gastos que realice el asegurado para la reparación de la contaminación o destrucción de datos de la empresa asegurada[80].

c) ***Costos de expertos para descubrir las causas de los daños o hackeo:***

Se amparan las erogaciones realizadas por el asegurado para analizar las causas del hackeo y la forma en que se introdujeron en su sistema, como asimismo la adopción de medida preventivas para evitar que se reitere la intromisión.

d) ***Extorsión:***

Por medio de esta cobertura se cubren las *extorsiones* que pueden producir los *hackers* exigiendo sumas de dinero[81] para no destruir o desen-

79 Burne, Katy - Sidel, Robin; *"Hackers found holes in Bank Network"*, en el Diario *'The Wall Street Journal'*, donde explican los robos de dinero que se produjeron en distintos Bancos en distintos lugares del mundo, como por ejemplo el Banco Central de Bangladesh, publicado con fecha 1° de Mayo de 2017.

80 Lanterman, Mark; *"Understand the layers of Cyber-Security and what data needs protecting"*, publicado en *'IRMI Expert Commentary'* del mes de Marzo de 2017.

81 Tuttle, Hilary; *"10 Cyberthreat Predictions for 2016"***,** en especial *"Ransomware"*, donde explica *"...38 % of organizations have already been targeted by cyberextortion, and the number of 'families'*

criptar información, como sucedió en el ataque global de fecha 12 de Mayo de 2017.

En efecto, a través del *ransomware*[82] que se produjo hace pocos días, los *hackers* exigían a las empresas y/o particulares que se pague un *rescate* en *Bitcoins* para que puedan volver a utilizar sus sistemas y tener acceso a sus archivos[83].

e) ***Denegación de Acceso:***

Otro de los riesgos que tienen las empresas, es que los *hackers* realicen una *denegación a acceso (D.O.S. Denial of services)*[84], en virtud del cual el asegurado no puede acceder a internet, sus páginas web, sus correos electrónicos, etc.

f) ***Business Interruption:***

f.1) En términos generales, la cobertura de *Business Interruption* es una de las más importantes para las empresas en general, dado que es un amparo amplio y dinámico que se otorga al asegurado.

Así, en el caso que una empresa tenga un siniestro habitual (por ejemplo: incendio), es que si la Compañía de Seguros paga inmediatamente la indemnización, es que muy posiblemente la empresa siniestrada tenga otros perjuicios, como son los *gastos fijos* que se producen hasta que se vuelvan a construir o reparar los bienes siniestrados; el *lucro cesante* por no poder trabajar normalmente, etc.

f.2) En estos casos es donde toma una trascendencia fundamental la cobertura de *Business Interruption*, dado que le pueden brindar distintas

of this type of malware grew more tan 600 % last year…", página 10, publicado en la Revista *"Risk Management",* Nueva York, del mes de Marzo de 2016.

82 Valach, Anthony; *"What to do after a Ransomware Attack"*, publicado en la Revista *'Risk Management'* Volume 63, Issue 5, página 12, del mes de Junio de 2015.

83 Granero, Horacio; *"Cómo prevenir un ataque de ransomware (leyendo el Art. 1.757 del Código Civil y Comercial)"*, publicado en 'El Dial', Cita: DC2321, de fecha 16 de Mayo de 2017.

84 Healy, Daniel - Palley, Stephen; *"Internet Down ? Insurance may cover your losses after a Denial of Service Attack"*, donde señalan las coberturas que existen *"…under a variety of cyber insurance policy forms, including network liability coverage that specifically cover DDoS attacks…",* publicado en Anderson Kill *"Policyholder Avisor & Alert"*, de fecha 25 de Octubre de 2016.

coberturas a la empresa asegurada, como el pago de los *gastos fijos*, la *pérdida de beneficios*, etc.

Incluso, también es conveniente tener contratada la cobertura de *Interrupci*ón de Negocios de carácter de *"Contingente"*, es decir, donde no es necesario que el daño se le ocasione al *propio asegurado*, sino que también va a tener cobertura de la *pérdida de beneficios* en los casos que la causa que genere dicha pérdida se la produzca a un *Proveedor* o un *Cliente*[85].

f.3) Y, la importancia de esta cobertura de *Business Interruption* se convierte en indispensable en los casos de *Cyber Risk*, dado que –por ejemplo– un *ransomware* o *denial of service (D.O.S.)*, etc., que genere una *interrupci*ón de negocios, puede producir pérdidas económicas de gran magnitud[86].

Con relación a la cobertura de *Business Interruption* en general, en varias pólizas de seguros, se requiere la existencia de un *daño a bienes tangibles*, como –por ejemplo– sucede en los casos de incendio, etc.

Corresponde destacar que en los casos de *Business Interruption* y de *Business Interruption 'Contingente'*[87] (que en algunos se ampara con un *sublímite)*[88] de los Seguros de *Cyber Risk* es que dicho requisito no se exige, dado que en la gran mayoría de los casos, van a tratarse de daños

85 Zola, Jared; *"Swatch fire losses and Contingent Business Interruption Coverage"*, publicado en *Insurance Journal*, de fecha 30 de Diciembre de 2015.

86 Una de la tantas Cláusulas de *"Cyber Business Interruption"*, que se utiliza a nivel internacional, reza:

"...We will insure you for your income, including where caused by damage to your reputation, and any increased cost of working, resulting solely and directly from an interruption to your business commencing during the period of insurance and lasting longer than the time excess, due to:

(a) *the activities of a third-party who specifically targets you alone by malicious blocking electronically the access to your computer system programmes or data you hold electronically; or*
(b) *a hacker who specifically targets you alone…".*

87 Ver: *"Purchasers Guide to Cyber Insurance Products"*, publicación del *"Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security"*, donde se explica *"...while some policies cover contingent business interruption (i.e. a cyber incident at a third party causes a business interruption for the policyholder), the sublimit for such coverage usually is very limited...",* publicado en el año 2016.

88 Downs, Andrew B.; en *Property Insurance Litigator's Handbook*, bajo la Coordinación de Leonard E. Murphy; Andrew B. Downs and Jay M. Levin; Capítulo 1.03 *'General Structure of the Property Insurance Policy'*, página 16 apartado (i) *"Policy Limits and Sublimits"*, American Bar Association, Chicago, Estados Unidos, 2007.

al *software*, o un denegación de acceso (D.O.S.), o una extorsión de un hacker, etc.[89].

f.4) Atento las limitaciones del presente trabajo, es que no profundizaremos las pautas de cobertura del *Business Interruption*, de manera tal que tan solo señalaremos que en principio existen dos (2) maneras principales de calcular las pérdidas, a través del: (i) *Gross Earning,* generalmente en las Pólizas norteamericanas; y (ii) *Loss of Profit*, comúnmente utilizadas en las coberturas europeas.

Así, en términos generales, se puede decir que en el amparo de *Gross Earning*, se suele otorgar cobertura indemnizatoria hasta que se vuelve a reparar o construir el bien dañado o el problema que genera el perjuicio[90].

En cambio, en la cobertura de *Loss of Profit,* habitualmente se extiende la indemnización hasta que se recupere el nivel de facturación que existía previa al siniestro (y siempre dentro del *plazo* de indemnización que se establezca en la póliza de seguros)[91].

6.1.2. Algunas de las diferencias que puede pueden existir entre los *Seguros 'Tradicionales'* y los *Seguros de 'Cyber Risk'* en *Daños Patrimoniales (Property):*

Según señaláramos *ut supra* en el mercado hay muchos textos de *Cláusulas y Condiciones* de Seguros de *Property* de *Cyber Risk*[92] y también hay distintas versiones de los seguros habituales de *Daños Patrimoniales*.

89 Freedman, Anne; *"Cyber Business Interruption: attacks on internet infrastructure commence, leaving unknown risks for insureds and insurers alike"*, publicado en *'Riskandinsurance'* de fecha 7 de abril de 2017.

90 Torpey, Daniel - Lentz, Daniel - Barret, David; *"The Business Interruption Book (Coverage, Claims and Recovery)*, Chapter 1: *"Insuring Changing Exposures"*, donde se explica con relación a la cobertura de *"Gross Earning"* que *"…that loss is covered only for the time required 'with the exercise of due diligence and dispatch' to repair, rebuild, or replace the damaged property from which the interruption arises…"*, página 11, Editorial The National Underwriter Company, Estados Unidos, Ohio, 2004.

91 Freedman, Anne; *"Cyber Business Interruption: attacks on internet infrastructure commence, leaving unknown risks for insureds and insurers alike"*, donde bajo el título *"Low Limits or Lack of coverage"* se señala con relación a *Business Interruption* y *Contingent Business Interruption* que *"…typically, policies provide 60 to 90 days as the period of restoration…"*, publicado en *'Riskandinsurance'* de fecha 7 de abril de 2017.

92 Middleton, Kirsty and Kazamia, María; *"Cyber Insurance: Underwritting, Scope of cover, Benefits and Concerns"*, en *The 'Dematerialized' Insurance*, bajo la Dirección de Pierpaolo Marano, Ioannis Rokas y Peter Kochenburger, Parte III, páginas 185 y siguientes, Editorial Springer, Suiza, 2016.

Sin perjuicio de ello, en términos generales, en forma asaz resumida, trataremos de establecer algunas de las diferencias que existen entre ambas coberturas.

 # Hackers

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

 # Amenzas y Extorsión:

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

 # Virus:

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

 # Pérdida de la Información de los Registros Informáticos:

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

 # Fraude Informático

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

 # Infidelidad de Empleados:

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

 # Business Interruption (por Denegación de servicio –D.O.S.–):

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura[93]

6.2. Cobertura de *Liability (Responsabilidad Civil):*

6.2.1. Coberturas de *Responsabilidad Civil (Liability)* en el Seguro de *Cyber Risk:*

Entre algunas de las coberturas[94] del Seguro de *Liability*[95] podemos mencionar las siguientes:

Responsabilidad por *datos personales*

Responsabilidad por *datos corporativos*

Responsabilidad por *empresas contratadas*

Otras Responsabilidades

a) **Responsabilidad por *datos personales:***

Se cubre a la empresa asegurada por las eventuales responsabilidad legales que puede llegar a tener por la publicidad o divulgación de *datos personales* de empleados, clientes, etc.

---

93 Gerking, Tyle - Smith, David; *"Insurance when the Internet goes down"*, donde señalan *"...a few insurers are now starting to broaden the business interruption coverage by changing the definition of 'computer system' or 'system' for purposes of business interruption coverage to include not just the insured's own network, but also the hardware and systems owned by thrid-party providers to which the insured is connected by a network (which includes the internet..."*, publicado en la Revista *"Risk Management"*, página 16, Volume 64, Issue 1, New York, de fecha Enero / Febrero de 2017.

94 Sobrino, Waldo - Gava, Adriel - Tortorelli, Mercedes (Directores); *Ley de Seguros Comentada*, Art. 109*,* publicada en www.laleyonline.com.ar

95 Entre varias cláusulas de *Responsabilidad Civil ('Media Liability')* que en la actualidad se comercializan a nivel mundial, se puede citar la siguiente, donde se cubren las responsabilidades derivadas de:

(a) *infringement of any intellectual property rights*
(b) *defamation, including libel, slander, trade libel, product disparagement or malicious falsehood; or*
(c) *negligent transmission of a virus*

which directly arises from the content of your email, intranet, extranet o website, including alterations or additions made by a hacker, we will indemnify you against the amount agreed by you and us through good faith negotiation, mediation or some other form of alternative dispute resolution to settle a claim or the amount to satisfy a judgment or arbitration award against you, including any judgment or award ordering you to pay claimant's lawyers' fees and costs...".

b) **Responsabilidad por *datos corporativos:***

Vinculado con el tema anterior, también se puede otorgar cobertura por la fuga de información de *clientes corporativos* del asegurado[96].

Así, si bien los Bancos, Compañías de Seguros, las empresas de Tarjetas de créditos, etc. son los casos típicos, es que no se debe perder de vista otros ejemplos, como los Contadores y/o Abogados y otros profesionales que también podrían ser demandados, por divulgación de *información confidencial* de sus clientes corporativos (como podría ser la fuga de información en un caso de compra o fusión entre empresas, etc.)[97].

c) **Responsabilidad por *empresas contratadas:***

También se otorga cobertura para aquellos casos de responsabilidad de la empresa asegurada[98], en los casos de divulgación de información de sus clientes, empleados etc., cuando la misma se encuentra almacenada[99] en otra empresa contratada[100], como podría ser –por ejemplo– en la *nube*[101, 102].

96 Ver: *"Purchasers Guide to Cyber Insurance Products"*, publicación del *"Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security"*, donde se estudia la *exclusión de cobertura* de *"Damages to Corporate Clients",* publicado en el año 2016.

97 Patterson, Mike; *"Improving Mergers & Acquisitions IT Security Practices"*, publicado en la Revista *'Risk Management'* Volume 63, Issue 5, página 8, del mes de Junio de 2015.

98 Raptis, Steve; *"Analyzing Cyber Risks Coverage"*, donde expone que *"…if a company uses the services of a third-party vendor to maintain its confidential customer or employee information in the 'cloud' and the vendor experiences a data breach, the company could be sued by its customers or employees, and may not have any coverage…",* publicado en *"Risk and Insurance"*, de fecha 13 de Marzo de 2015.

99 Gold, Joshua - David Wood; *"Cyber Claims Insurance Protection is a Tricky Business",* donde bajo el título de *"Cover Cloud and Third Party Vendors"*, donde se expone *"…make sure that your cyber-specific coverage protects againts losses where others manage, transmit or host data for your company…"*, agregando *"…insurance coverage is available for cloud computing and instances where data is handled, managed or outsourced to a third party…",* publicado en *"Enforce"* de fecha 20 de Noviembre de 2015.

100 Tuttle, Hilary; *"10 Cyberthreat Predictions for 2016"*, en particular *"Hacking the Cloud"*, página 11 publicado en la Revista *"Risk Management"* del mes de Marzo de 2016.

101 Ver: *"Purchasers Guide to Cyber Insurance Products"*, publicación del *"Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security"*, donde se analiza el tema de *"Information maintained and stored by third parties"* publicado en el año 2016.

102 Gold, Joshua; *"10 Tips to Maximize Cyber Insurance Recovery",* donde explica que se debe tener especial cuidado cuando el asegurado tiene almacenada o procesa información a través de terceras empresas o utiliza la *nube (Cloud),* señalando *"…there are insurance coverage implications if you use 'cloud computing' or other vendors for hosting and processing data…",* publicado en Anderson Kill *"Policy Advistor & Alert"*, de fecha 1° de Octubre de 2014.

d) ***Otras Responsabilidades:***

Es importante señalar la gran cantidad de situaciones, por las cuales una empresa asegurada puede ser objeto de un reclamo por responsabilidad son innumerables[103].

Por un lado, es básico señalar que en los temas de *cyber risks*, en muchos casos existe una íntima relación entre las cuestiones de *Property* y *Liability*, dado que la producción de un siniestro de *Daños Patrimoniales*, además de generar un perjuicio al propio asegurado, también puede llegar a tener consecuencias sobre otras empresas (generando el pertinente reclamo de *responsabilidad civil*).

Así, por ejemplo, un siniestro de *Property* derivado de *Hackers; Extorsión; Pérdida de la Información de los Registros Informáticos; Fraude Informático; Infidelidad de Empleados;* etc. también puede producir *daños y perjuicios a terceros* (que se debe amparar por la cobertura de *Liability*).

Incluso, algunos de dichos daños podrían estar amparados por el seguro de la propia empresa damnificada, por ejemplo, teniendo una cobertura de *Business Interruption 'Contingente' (por Denegación de servicio –D.O.S.–*)[104], pero luego hasta podría existir una *acción de recupero* de la Compañía de Seguros que abonó dicho siniestro a la empresa damnificada[105].

Asimismo, también se deben amparar las responsabilidades legales de la empresa asegurada ocasionadas por medio de la página web, intranet, correo electrónico[106], etc., como por ejemplo:

103 Beecher Carlson; *"Cyber: a Tale of two markets" (Inconsistencies in Cyber insurance policies can lead to 'Swiss cheese towers' of coverage)"*, donde se expone que *"...non-traditional risks such physical damage and bodily injury resulting form cyber breach or system failure pose new threats and challenges..."*, publicado en *Risk & Insurance* con fecha 15 de de Marzo de 2017.

104 Gerking, Tyle - Smith, David; *"Insurance when the Internet goes down"*, donde señalan *"...a few insurers are now starting to broaden the business interruption coverage by changing the definition of 'computer system' or 'system' for purposes of business interruption coverage to include not just the insured's own network, but also the hardware and systems owned by thrid-party providers to which the insured is connected by a network (which includes the internet..."*, publicado en la Revista *"Risk Management"*, página 16, Volume 64, Issue 1, New York, de fecha Enero / Febrero de 2017.

105 Ver: *"Firms hit by Cyber attack could face lawsuits over lax security: Legal Experts"*, publicado en *'Insurance Journal'*, de fecha 16 de Mayo de 2017.

106 Carbone, Carlos; *"Los modernos soportes de correspondencia en el Código Civil y Comercial"*, publicado en el Diario 'La Ley', de fecha 10 de Marzo de 2017.

infracción de *derechos de autor, nombres de dominio, marca.*

difamación, calumnias, falsedades, etc.

violación de derechos de *propiedad intelectual*

robo físico de hardware (v.gr. notebooks; smartphones, tablets, etc.) donde se encontraren datos almacenados[107]

transmisión de *virus*[108]

denegación de acceso a datos por parte del cliente o de un tercero autorizado

daños o destrucción de *datos almacenados*

revelación y/o divulgación de datos[109]

6.2.2. Algunas de las diferencias que puede pueden existir entre los *Seguros 'Tradicionales'* y los *Seguros de 'Cyber Risk'* en *Responsabilidad Civil (Liability):*

 # Daños Patrimoniales Puros:

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

 # Difusión de Datos Privados:

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

107 Gold, Joshua; *"10 Tips to Maximize Cyber Insurance Recovery"*, donde señala que al tratarse de un riesgo muy importante para la empresa asegurada y como en muchas pólizas de seguros se encuentra excluído de cobertura, es que determina *"...make sure that your insurers covers breaches arising forn* ***mobile devices*** *that may or may nor connected to the company's computer network...",* publicado en Anderson Kill *"Policy Advistor & Alert"*, de fecha 1° de Octubre de 2014.

108 Raptis, Steve; *"Analyzing Cyber Risks Coverage"*, publicado en *"Risk and Insurance"*, de fecha 13 de Marzo de 2015.

109 Keegan, Chris, *"Cyber Insurance covered by T.R.I.A."*, publicado en *Beecher Carlson Insurance Services*, del mes de Enero de 2017.

 # Denegación de Servicio (DDoS):

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

 # Fraude Informático:

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

 # Virus informáticos:

Seguros *tradicionales:* no brindan cobertura

Seguros *cyber risk:* si otorgan cobertura

CONCLUSIONES

Como corolario de todo lo antes desarrollado, podemos finalizar señalando que:

1) El Ciberataque mundial de fecha 12 de Mayo de 2017, si bien fue uno de los primeros a nivel global, es que no será el último, dado que dichos *ciberataques* se convertirán en algo normal y habitual.

2) Nos encontramos frente a un verdadero *Tsunami Tecnológico* que nos obliga a abrir la mente para tratar de internalizar los nuevos escenarios.

3) A nivel legal, se abre un panorama novedoso respecto a los *Daños Patrimoniales* y –muy especialmente– en el ámbito de la *Responsabilidad Civil.*

4) Los Seguros de *Cyber Risk* son una herramienta indispensable y fundamental para las empresas aseguradas, que les puede otorgar cobertura en muchas situaciones donde existen riesgos.

5) En el Seguro de *Cyber Risk* no existe *wordings* estándar, por lo cual las Compañías de Seguros y los Productores de Seguros y los

Brokers de Seguros, deberán profundizar el *Deber de Información*[110], el *Deber de Consejo* y el *Deber de Advertencia*[111].

6) Asimismo, las empresas aseguradas deberán analizar en profundidad las Cláusulas y Condiciones de los Seguros de *Cyber Risk*, para estudiar si amparan los riesgos que quieren cubrir.

110 Sobrino, Waldo; *"El 'Deber de Información', de 'Consejo' y de 'Advertencia' en materia de Seguros"*, en especial, Capítulo VIII *"El Deber de Consejo",* publicado en el Diario 'La Ley', página 2, de fecha 1° de Febrero de 2017.

111 Sobrino, Waldo; *Seguros y el Código Civil y Comercial (y su relación con la Responsabilidad Civil, el Derecho del Consumo, la Constitución Nacional y los Tratados Internacionales)***, Capítulo .IX.1)** *"El 'Deber de Información: y su relación con el 'Deber de Prevención', el 'Deber de Precaución', el 'Deber de Consejo' y el 'Deber de Advertencia'"*, páginas 445 a 488, Editorial La Ley, Julio de 2016.