Informe de objetivos
August 17, 2018

El Mercado de los Ciberseguros: Pruebas de Estrés para el Futuro

Dadas las perspectivas de riesgo idiosincrásico y desafíos de agregación sistémica, las aseguradoras han adoptado un enfoque moderado y conservador para la suscripción de riesgos cibernéticos

La creciente velocidad de los avances tecnológicos ha modificado profundamente los procesos de negocios, las cadenas de suministro y los mecanismos de entrega a través de un número de industrias: los sistemas universitarios, de salud, entretenimiento, transporte y finanzas. Tanto la acumulación de datos, como la tecnología que los utiliza, se han vuelto con el tiempo, significativamente más sofisticados, mientras que los controles de infraestructura de datos y seguridad no han logrado mantenerse a la par. No hay una cantidad de dinero que una empresa pueda pagar para mantenerse 100% a salvo, de manera que los seguros resultan un complemento natural a los esfuerzos por mitigar las pérdidas, para proporcionar respaldo financiero en el caso de un siniestro. Tradicionalmente, la industria de los seguros ha reaccionado de manera lenta a la innovación tecnológica, pero se encuentra en una posición única al administrar este riesgo emergente, pues compete a su propio negocio y a los de sus asegurados.

El riesgo cibernético es distinto al resto de los riesgos, lo que obedece a factores como la falta de datos actuariales, su rápida evolución y amplio alcance operacional que incluye gente, procesos, tecnología, y potenciales adversarios activos. La naturaleza idiosincrática de este riesgo es difícil de estimar y se encuentra en clara expansión, con pérdidas significativas recientes para los servidores de las compañías más grandes del mundo, incluyendo a Target, Home Depot, J.P. Morgan Chase, Equifax, Anthem, Yahoo y Sony.

El riesgo idiosincrático se puede administrar a través de la diversificación, límites de riesgo y operaciones de suscripción prudentes, pero el riesgo cibernético presenta nuevos retos sistémicos también. Malware como NotPetya o interrupciones a proveedores de servicios clave como el ataque DDoS (Ataque de Denegación de Servicio Distribuido, por sus siglas en inglés) en servidores dinámicos puede afectar a múltiples asegurados, causando una pérdida agregada a las aseguradoras. Las aseguradoras son conservadoras con respecto a asegurar riesgos cibernéticos, por lo tanto, el enfoque que han puesto en la suscripción de éstos ha sido mesurado: han asignado un porcentaje muy pequeño de su portafolio general de seguros al riesgo cibernético, con asignaciones típicas de primas de menos del 1%. En adición a esto, los límites ofrecidos en los ciberseguros han sido más bien bajos, en comparación con los riesgos ya bien entendidos, como el riesgo de daños catastróficos a la propiedad, para prevenir pérdidas individuales significativas de las empresas.

Con el crecimiento del mercado del ciberseguro, probablemente las aseguradoras retendrán mayores porcentajes de riesgo inherentes a las operaciones de suscripción. Aunado a esto, las implicaciones del riesgo cibernético se extienden más allá del mercado de seguros. Los siniestros cibernéticos también pueden causar pérdidas silenciosas, donde las pólizas suscritas para cubrir otro tipo de siniestros como daños a la propiedad, D&O (directores y oficiales), y E&O (errores y omisiones), tienen cobertura contra pérdidas causadas por un peligro cibernético. En adición a la exposición que las aseguradoras enfrentan por parte de sus operaciones de suscripción, éstas también están directamente expuestas a riesgos operativos, pues las operaciones de los negocios dependen fuertemente de los sistemas de tecnología de información, debido a que las transacciones de alta seguridad y disponibilidad son un requerimiento para un buen servicio al cliente y para construir confianza y reputación dentro de un mercado saturado.

Contacto de Analistas:
Fred Eslami, Oldwick
+1 (908) 439-2200 Int. 5406
Fred.Eslami@ambest.com

Sridhar Manyem, Oldwick
+1 (908) 439-2200 Int. 5612
Sridhar.Manyem@ambest.com

Contribución:
Bobby Skrabal, Oldwick

SR-2018-074

Anexo 1

Industria de Daños en E.U.A - Top 20 de Primas Emitidas Directas de

2017 Rango	2016 Rango	Nombre de la Compañía	2017 PED	2016 PED	% de PED de Ciberseguridad en 2016 Indivuduales	% de PED de Ciberseguridad en 2016 Grupales
2	1	American International Group	227.6	228.3	100.0	0.0
3	2	XL CatlinAmerica Group	177.9	160.8	100.0	0.0
1	3	Chubb INA Group	284.4	133.6	26.4	73.6
4	4	Travelers Group	119.1	92.2	71.7	28.3
5	5	Beazley Insurance Company, Inc.	95.0	83.9	90.3	9.7
6	6	CNA Insurance Companies	73.1	68.5	34.7	65.3
9	7	Liberty Mutual Insurance Companies	60.0	56.4	57.7	42.3
7	8	BCS Insurance Company	69.9	55.4	58.1	41.9
8	9	AXIS Insurance Group	63.8	50.3	73.5	26.5
21	10	Allied World Assurance Group	19.7	32.5	99.6	0.4
11	11	Tokio Marine US PC Group	40.0	30.6	99.0	1.0
10	12	Zurich Financial Services NA Group	43.0	26.2	98.8	1.2
16	13	Berkshire Hathaway Insurance Group	28.8	26.1	42.9	57.1
14	14	Sompo Holdings US Group	31.7	25.2	8.8	91.2
13	15	Hartford Insurance Group	34.9	25.0	19.3	80.7
22	16	Markel Corporation Group	14.5	24.4	100.0	0.0
20	17	Alleghany Insurance Holdings Group	15.8	15.5	75.9	24.1
19	18	Starr International Group	17.2	12.9	78.7	21.3
25	19	Great American P & C Insurance Group	13.5	12.3	68.8	31.2
23	20	Hiscox USA Group	14.5	11.1	85.1	14.9
		Total de la Industria de Daños	**1,810.7**	**1,341.5**	**67.9**	**32.1**

* Clasificados según el total de sus primas emitidas directas de ciberseguridad, individuales y grupales en 2016. PED en millones de dólares.

Fuente: Datos e investigación de A.M. Best

Un Salto Hacia Adelante: El Mercado de los Ciberseguros en 2022

Dado el increíble crecimiento y estado dinámico del mercado cibernético afirmativo, A.M. Best, en conjunto con el equipo de Análisis de Riesgo de Guidewire Cyence, condujeron una prueba de estrés sobre el top 20 de proveedores de ciberseguros (aseguradoras) del 2016 (Anexo 1) para analizar las implicaciones potenciales de que una catástrofe cibernética ocurriera. La lista incluye algunas de las aseguradoras más importantes a nivel global, que podrían tener una mayor exposición al riesgo dado su participación de mercado, en la creciente área de cobertura.

Escogimos proyectar el mercado de ciberseguros a 2022, para permitir que emergiera un portafolio en estado estable. Dado que el mercado de los seguros cibernéticos está visiblemente en constante flujo, una prueba a mayor plazo estaría sujeta a una incertidumbre considerable.

Proyectando el Mercado de Seguros

Para este ejercicio, promediamos los índices de crecimiento históricos de la industria, así como las proyecciones a futuro de distintas fuentes de la industria, y fijamos una tasa anual de crecimiento de 28%. Esto puede parecer conservador, considerando que los riesgos cibernéticos le cuestan a los Estados Unidos el 1% de su producto interno bruto, cerca de 800 mil millones de dólares al año, y el mercado de la seguridad cibernética está por encima de los 100 mil millones de dólares. Entre las causas que son específicamente relevantes para el crecimiento continuo del mercado de los seguros cibernéticos, se encuentran las siguientes cuatro:

Suplemento de la Asociación Nacional de Comisionados de Seguros

La información propuesta en este reporte se basa en el Suplemento de la Cobertura de Seguros de Ciberseguridad y Robo de Identidad, introducido inicialmente por la Asociación Nacional de Comisionados de Seguro (NAIC, por sus siglas en inglés) al final del 2015. El suplemento está desglosado en base a la cobertura de los seguros, que pueden ser individuales o grupales. Para las pólizas grupales, se requirió que las compañías proporcionaran un monto que pudiera ser verificado, o bien, un estimado para las pólizas grupales. Esta información se limita a las compañías que archivan sus estados financieros anuales con NAIC. A.M. Best hace notar que el suplemento sólo se publicó en 2015, por lo tanto, los datos tienen ciertas limitaciones.

- Pequeñas y medianas empresas: Se estima que las tasas de elegibilidad de seguros cibernéticos para las Pymes se encuentran en un intervalo que va del 5% al 25%. Los datos del 2017 del Sistema Norteamericano de Clasificación de Industrias (NAIC, por sus siglas en inglés), identifica apenas 2.5 millones de pólizas cibernéticas colocadas en los Estados Unidos – solamente alrededor del 8% de los 29.6 millones de empresas estimadas, según datos del 2014 de la Oficina del Censo de los Estados Unidos. De acuerdo con Advisen, entre 2011 y 2015, las tasas de elegibilidad del sector de las Pymes crecieron más rápido que los de cualquier otro, y aún hay suficiente espacio para más crecimiento. Varios líderes de mercado como AIG, Liberty Mutual y Hartford han dado a conocer sus intenciones de enfocarse en el mercado de las Pymes.
- Sector de la industria en expansión: En un mundo cada vez más interconectado y dependiente de la tecnología, los riesgos cibernéticos se presentan en múltiples formas para todas las industrias. Hoy en día, las pólizas cibernéticas han respondido a estas necesidades mediante estructuras versátiles que son capaces de cubrir un rango de exposición, que incluye costos por violación de datos del cliente, responsabilidades, extorción en línea e interrupción de los negocios. Adicionalmente, los agentes de seguro pueden personalizar la cobertura, abordando las brechas que existen en las pólizas cibernéticas tradicionales y líneas convencionales, como crimen o daños a la propiedad, lo que facilita su adopción en industrias como la manufacturera o de servicios públicos.
- Ámbito internacional: las organizaciones domiciliadas en Estados Unidos, constituyen un estimado del 90% de las primas emitidas brutas de ciberseguros al día de hoy. Esto difiere significativamente de otras líneas de cobertura para pólizas de daños, para las cuales, E.U.A. solo representa el 40% de las primas brutas emitidas. El mercado de los seguros cibernéticos de los Estados Unidos despegó cuando la Ley de violación de datos personales y otras leyes de privacidad se implementaron; esto resalta los costos tangibles asociados a la violación de datos. Estas legislaciones ahora proliferan a nivel global; o bien ya han sido establecidas, o lo serán en el corto plazo en Canadá, la Unión europea, Reino Unido y Australia, entre otros países.
- Límites, exposición y precios al alza: De acuerdo con Marsh, que ha publicado tendencias límite para todos sus clientes de 2012 a 2015, el crecimiento promedio en los límites durante este el período fue 15.8% anual. Extrapolando al 31 de diciembre de 2022, esperamos que los límites de compra promedio de una empresa se dupliquen. El Índice Global de Mercado de Seguros Marsh ha rastreado cambios en las tasas de las pólizas de ciberseguros desde 2012, y muestra un cambio anual promedio en la tasa del 5.2%, que contrasta marcadamente con la tasa de renovación de los seguros contra accidentes, del -0.6%, durante el mismo periodo.

Generando Portafolios Cibernéticos para 2022

Para este informe, A.M. Best y Cyence modelaron los ingresos de las compañías que podrían adquirir cobertura cibernética, así como las pólizas específicas que pueden comprar de compañías de seguros individuales. Nos enfocamos en aprovechar los conocimientos y datos de la industria, los informes de mercado y los informes públicos, para modelar el mercado

Anexo 2
Categorías de Perfil de Póliza Cibernética - 2017

	Descripción	Ingresos	Límites	Sub-límites	SIR	Adhesión
Cuentas Nacionales –– Enfocadas	Cuentas con ingresos superiores a 10 mil millones de dólares, con puntos de conexión primarios o de bajo excedente (generalmente, menos de 50 millones de dólares)	10 mil millones de dólares	10 millones de dólares	50%	5 millones de dólares	6.5 millones de dólares
Cuentas Nacionales – Exceso	Cuentas con ingresos superiores a 10 mil millones de dólares, con un mayor exceso de puntos de embargo (generalmente, entre 50 y 250 millones mdd)	10 mil millones de dólares	10 millones de dólares	50%	5 millones de dólares	100 millones de dólares
Mercado Medio Suscrito	Empresas con ingresos superiores a 500 millones de dólares que son predominantemente primarios, pero también tiene un bajo exceso	500 millones de dólares	3 millones de dólares	33%	500 mil dólares	750 mil dólares
PyMEs – Individuales	Empresas con ingresos menores a 500 millones de dólares que son predominantemente primarios	25 millones de dólares	1 millón de dólares	25%	15 mil dólares	N/A
PyMEs – Grupales	Empresas con ingresos de menos de 500 millones que son primarias y están suscritas como un respaldo a otra póliza como un BOP o CGL	25 millones de dólares	100 mil dólares	25%	10 mil dólares	N/A

Fuente: Datos e Investigación de A.M. Best

en general y ampliar nuestros hallazgos al nivel de póliza, utilizando cinco perfiles típicos de póliza (Anexo 2). Este enfoque nos permite ampliar los índices de elegibilidad e ingresos de la industria, para traducirlos a límites de póliza específicos, adhesiones, retenciones, sublímites, etc., que una aseguradora puede colocar para una compañía.

Las carteras de las 20 principales aseguradoras cibernéticas, según sus primas emitidas brutas, se modelaron mediante la asignación de proporciones de cada perfil de póliza a cada cartera de aseguradora agregada, comparando los informes del mercado de ciberseguros de 2016 con respecto al número de pólizas, las primas emitidas totales y las proporciones de seguros individuales y grupales. Al seleccionar compañías específicas y su cobertura cibernética afirmativa asociada (límites, retención pactada de autoaseguramiento, etc.) para crear carteras específicas de aseguradoras, extrajimos las distribuciones para cada elemento que tenía un valor medio que coincidía con la categoría de perfil de la póliza, para permitir que hubiera variación.

Enfoque de Modelado y Pruebas de Estrés

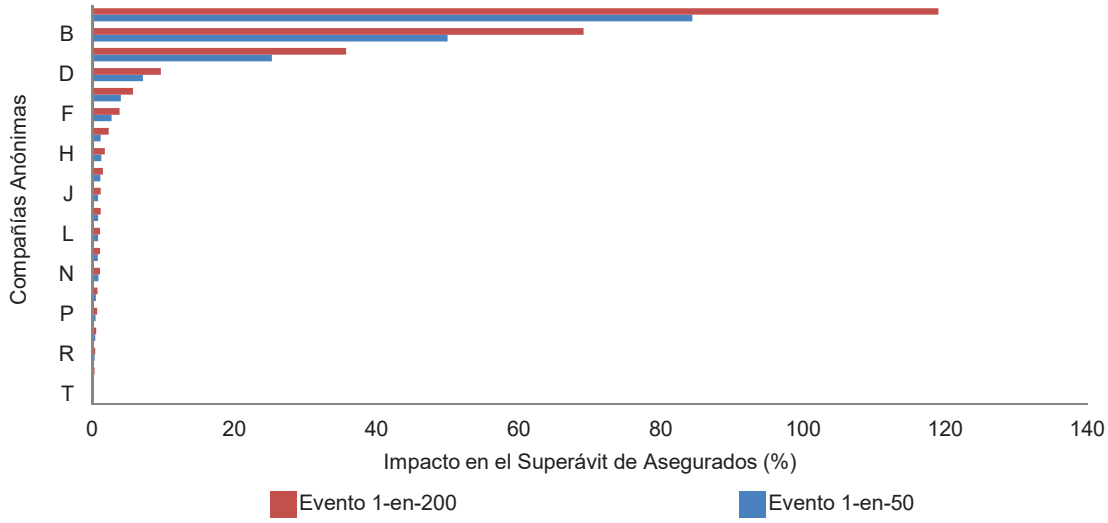
Con las carteras de las 20 principales aseguradoras cibernéticas modeladas a 2022, Cyence aprovechó su aplicación de análisis de riesgo para modelar las pérdidas. El "motor de escucha de datos" de Cyence recopila datos acumulados y de exposición real, para un universo de empresas. Aprovechando técnicas avanzadas de modelado, como el aprendizaje automático, Cyence puede correlacionar los atributos de la empresa con incidentes pasados, identificar tendencias y proyectar la exposición cibernética en términos de dólares y probabilidades. El modelo de pérdida estocástica de Cyence conduce miles de simulaciones de Monte Carlo, introduciendo variaciones a través de múltiples entradas para generar una distribución de probabilidad de excedencia de la pérdida esperada. Este informe se centra en los períodos de retorno de 1 en 50 y 1 en 200, que se han convertido en puntos de referencia comunes en la industria, y representan un potencial de pérdida grave pero plausible, para la evaluación de la adecuación de capital.

La aplicación Cyence permitió la evaluación de las 20 carteras cibernéticas modeladas de las 20 aseguradoras principales, en varios escenarios, para modelar su potencial de pérdida. Dado que muchas aseguradoras reportan sobre escenarios de desastre realistas y específicos, consideramos que sería apropiado modelar en base a dos escenarios descritos en el informe de riesgo emergente de Lloyd en 2017, "Contando los costos: Decodificación de riesgo cibernético: una interrupción al proveedor de servicios en la nube y vulnerabilidad masiva". En el primer escenario, fallan numerosos servidores de clientes basados en la nube, lo que lleva a interrupciones generalizadas de servicios y negocios; en el segundo, una aplicación de software común se ve comprometida y explota a escala global. Estos escenarios representan solo dos de las muchas rutas de que tienen el potencial de causar eventos de acumulación

Anexo 3

Escenario de Vulnerabilidad Masiva

Clasificadas por las Pérdidas Esperadas Brutas en Relación con el Excedente de los Asegurados en el escenario 1 en 200

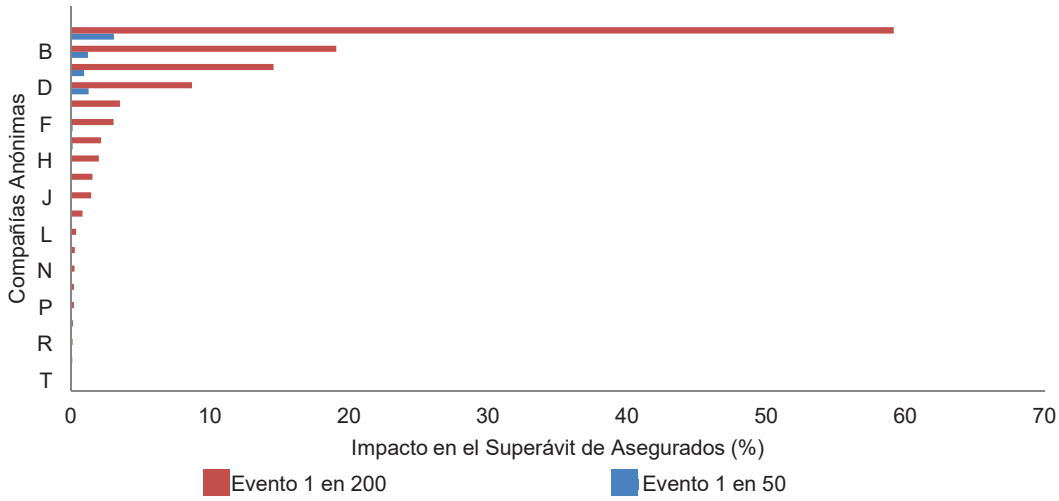


Fuente: Datos e Investigación de A.M. Best

Anexo 4

Escenario del Proveedor de Servicios en la Nube de Lloyd's

Clasificadas por sus Pérdidas Esperadas Brutas en Relación con el Excedente de Asegurados en un Escenario de 1 en 200



Fuente: Datos e Investigación de A.M. Best

cibernética. Para capturar la totalidad de las pérdidas potenciales, Cyence también modeló las pérdidas anuales totales de la cartera de todos los tipos de eventos. Los modelos estocásticos de Cyence nos permitieron examinar el potencial de pérdida en los niveles de severidad de pérdida por año de 1 en 50 y 1 en 200.

Resultados Afirmativos del Modelado de Pérdida Cibernética

En este ejercicio, tres de las empresas perdieron entre el 15% y el 119% de su superávit de asegurados estimado en 2022, en un escenario de evento único. Además de los dos escenarios de eventos, evaluamos las pérdidas anuales (de las pérdidas totales de las carteras) que podrían ocurrir durante un período de 12 meses como resultado de todos los eventos (Anexos 3 y 4). En el nivel de 1 en 200, cinco compañías incurrieron en pérdidas que oscilaron entre el 11% y el 233% de su superávit de asegurados de 2022.

Estas pérdidas modeladas son brutas y no incluyen el efecto neto del reaseguro. Según Aon Benfield, aproximadamente 525 millones de dólares en primas de reaseguro emitidas brutas se colocaron en 2015. La forma más común de reaseguro es el trato de quota share (cuota parte). Bajo ese esquema, quota share 50/50, una aseguradora primaria solo retendría la mitad de la pérdida modelada. El valor del reaseguro para mitigar estas pérdidas es crítico, pero, debido a la falta general de datos e información sobre los acuerdos de reaseguro, nuestra evaluación se centró en la pérdida bruta en lugar de hacer una inferencia sobre los posibles acuerdos de reaseguro que los aseguradores pueden tener.

Los resultados generales de las pruebas de estrés indican que las pérdidas de cartera son menores en relación con las exposiciones brutas a riesgos catastróficos de las compañías, medidas por sus pérdidas máximas probables (PML, por sus cifras en inglés).

Consideraciones Sobre la Pérdida Cibernética Silenciosa

Los mismos eventos asociados con las pérdidas cibernéticas afirmativas, también podrían ser parte de ataques cibernéticos dirigidos contra activos físicos, o simplemente podrían activar pólizas de seguro no cibernéticas. Por ejemplo, el ataque de malware NotPetya de 2017, aprovechó vulnerabilidades conocidas públicamente en sistemas operativos comunes, como Microsoft, y activó la cobertura de interrupción de negocios de muchas pólizas de propiedad. Este riesgo es especialmente preocupante, dado que los límites en los programas de propiedades multinacionales exceden significativamente lo que se ofrecería en el mercado de suscripción cibernética afirmativa estándar. Este tipo de ataques resaltan la omnipresencia de la exposición silenciosa al riesgo cibernético, así como el valor de contar con una estrategia para administrar la cobertura ofrecida, además de la selección y suscripción de riesgos, el uso de exclusiones y sublímites y la fijación de precios para el riesgo cibernético silencioso en estas pólizas.

Los escenarios descritos en este informe tienen como objetivo cuantificar las pérdidas máximas probables de las pérdidas cibernéticas afirmativas y directas únicamente. La cuantificación de las pérdidas máximas probables de los riesgos cibernéticos silenciosos, no se presta a modelos económicos generalizados, debido en parte a la sustanciosa ambigüedad contractual inherente. Aunque no modelamos tales pérdidas cuantitativamente en este ejercicio, éstas constituyen un componente crítico del riesgo cibernético para las aseguradoras.

Consideraciones de Pérdida Directa

Las compañías de seguros también tienen una exposición directa a los incidentes cibernéticos, debido en parte al volumen considerable de información sensible que manejan y al aumento en la dependencia de los sistemas de tecnologías de la información, con alta disponibilidad para potenciar las funciones críticas del negocio. Algunos de los incidentes cibernéticos más

grandes y más costosos han ocurrido en el sector de seguros. La violación de los sistemas de información de Anthem en enero de 2015, ofrece una perspectiva única. Esta violación involucró los registros financieros y de salud de más de 78 millones de clientes, y resultó en un acuerdo de 115 millones de dólares (después de un caso judicial de dos años), y 260 millones de dólares en gastos por mejoras de seguridad y remediación. Estas cifras de gastos directos divulgadas públicamente no son exhaustivas; no cubren pérdidas debido a la interrupción del negocio o las implicaciones reputacionales del incidente.

Nuestro modelo muestra que, para muchos de los principales mercados cibernéticos, los niveles de riesgo cibernético retenidos, a través de la suscripción, eclipsarán la exposición directa del propio asegurador para el año 2022. Sin embargo, los resultados fueron generalizados y las pérdidas directas de varias aseguradoras, superaron sus pérdidas aseguradas, a pesar del crecimiento afirmativo de la cartera cibernética modelada. Al igual que con nuestro modelo de pérdida afirmativa del ciberseguro, estos hallazgos no incluyen las recuperaciones potenciales del seguro, si la propia aseguradora tiene cobertura contra riesgos cibernéticos por su exposición directa a éstos.

Consideraciones Sobre la Calificación y la Administración Integral de Riesgos

En el análisis actual, las pérdidas brutas en los escenarios 1 en 50 y 1 en 200 para la mayoría de estas empresas no se acercan a las pérdidas máximas probables por catástrofes naturales, utilizadas para estresar la solidez del balance de las empresas. Sin embargo, hay un puñado de compañías que pueden perder una cantidad significativa de superávit, lo que podría presionar la calificación o provocar una baja en ésta. Sin embargo, debemos tener en cuenta, que estas pérdidas son brutas y no consideran los acuerdos de reaseguro en los que estas compañías pueden tomar parte. Este análisis tampoco tiene en cuenta la exposición silenciosa al riesgo cibernético que estas empresas pueden tener, lo que podría ser significativo. La falta de datos e información sobre el reaseguro y la exposición cibernética silenciosa nos llevan a considerar el riesgo cibernético en el marco de administración de riesgos de cada compañía.

A.M. Best ha desarrollado una serie de preguntas que las aseguradoras deben considerar al abordar la exposición derivada de pérdidas cibernéticas afirmativas, silenciosas y directas. La evaluación del riesgo cibernético como un peligro de este estilo, resulta en un rango de resultados con el potencial de impactar negativamente el balance de una aseguradora, incluso para aquellas que optan por no suscribir la cobertura cibernética afirmativa debido a la posibilidad de pérdidas aseguradas silenciosas, así como exposiciones directas.

Desde nuestro punto de vista, el objetivo de cualquier programa de administración de riesgos no es eliminar el riesgo, sino comprender, comunicar, gestionar y mitigar la volatilidad potencial. Los riesgos en evolución, como el cibernético, requieren un enfoque cuantitativo y cualitativo equilibrado, que comienza definiendo el apetito y la tolerancia al riesgo cibernético, y cómo éste encaja con la estrategia general de la aseguradora, las declaraciones de tolerancia del riesgo empresarial y los objetivos de solidez financiera y rentabilidad. La gestión de este riesgo debe ser sólida y la administración de la aseguradora, la gestión de riesgos, los equipos de suscripción e incluso la junta directiva, deben tener en cuenta la cantidad de riesgo que la aseguradora está dispuesta a asumir, así como las posibles pérdidas y el impacto que puede tener en la base de capital de la aseguradora y las ganancias.

Al igual que con cualquier mecanismo de gobierno, las comunicaciones sobre el riesgo cibernético deben ser bien articuladas, metódicas y frecuentes. Los informes de riesgo que toman en cuenta factores como los resultados de las pruebas de resistencia al estrés, los detalles de la exposición a los riesgos cibernéticos, el potencial de acumulación, los límites por sector, industria y la exposición de reaseguro, se consideran favorables. Estos informes deben

compartirse con los inversionistas y otras partes interesadas, como reguladores y analistas de A. M. Best, para que exista conciencia del potencial de pérdida y la volatilidad asociada con el riesgo cibernético.

La organización completa debe comprender las declaraciones y comunicaciones sobre el apetito de riesgo y deben incluir controles para garantizar que no se superen los límites de riesgo, además de los mecanismos para garantizar la comunicación y la gestión adecuadas de las infracciones en dichos límites. El diálogo continuo que evalúa estas situaciones a medida que cambia el riesgo es crítico.

Realizar una prueba de estrés para estos riesgos, con el fin de evaluar el impacto de los eventos de estrés en el balance de la empresa (para confirmar que la cartera cibernética no presenta tensiones de capital o rebajas en las calificaciones), y diseñar estrategias de mitigación de riesgo, como reaseguros, evasión o suposición (del riesgo), y ajuste de precios, serán aspectos clave de la revisión de Best sobre el enfoque de una aseguradora para gestionar el riesgo cibernético.

Muchas aseguradoras han notado que la falta de datos críticos, sobre proveedores externos y rutas de acumulación, presenta un desafío clave para su capacidad de administrar el riesgo cibernético. En ausencia de este tipo de información, las estrategias de suscripción deben centrarse en la gestión de límites, la diversificación por industria y el tamaño de los ingresos, y la selección juiciosa de riesgos. A medida que el mercado de los ciberseguros crezca y las aseguradoras retengan mayores cantidades de riesgo, a través de operaciones de suscripción, el uso de datos reales de exposición y la identificación de las rutas de acumulación, para asegurar la adecuación de los precios y una comprensión integral de la exposición, adquirirán un papel crítico.

Al igual que con las ofertas de cobertura afirmativa, el uso de datos de exposición real, para mejorar el conocimiento de la postura del riesgo respecto a la seguridad cibernética del asegurado, y las tendencias de riesgo cibernético, puede mejorar en gran medida la comprensión de las rutas silenciosas de acumulación cibernética, por parte de una aseguradora. Este conocimiento ayudaría a responder preguntas como las siguientes:

- Para cualquier línea de cobertura dada, ¿cuántas pérdidas esperamos ver en el próximo año detonadas por un “ciber gatillo”?
- ¿Cuál es el alcance de las pérdidas que podrían surgir de tales circunstancias?
- ¿Cuáles son las posibles vías de acumulación cibernética que nuestro proceso de suscripción existente no tiene en cuenta?

Las respuestas a estas preguntas permitirían evaluar el posible impacto marginal en la frecuencia y gravedad de las reclamaciones proyectadas, así como la identificación e investigación de posibles nuevos caminos de acumulación cibernética.

Los reguladores enfrentan desafíos similares a los que enfrentan las aseguradoras, firmas de modelado y agencias de calificación. En Reino Unido, la guía de la Autoridad de Regulación Prudencial (PRA, por sus siglas en inglés) sobre la gestión silenciosa de la pérdida cibernética, destaca específicamente la identificación de niveles de tolerancia aceptables para una cartera, con un impacto potencialmente alto en el riesgo cibernético, incorporando la identificación del riesgo y los procesos de gestión en la selección de riesgos y precios. La Asociación Nacional de Comisionados de Seguros (NAIC, por sus siglas en inglés) a finales de 2017, adoptó la Ley Modelo de Seguridad de Datos de Seguros, que establece los estándares para la seguridad e investigación de datos y notificación de un incumplimiento de la seguridad de datos, aplicable

a los proveedores de seguros. Tanto la NAIC (a través de la ley modelo) como el Departamento de Servicios Financieros de Nueva York (NYDFS, por sus siglas en inglés) se están enfocando en los datos y las prácticas de seguridad de las aseguradoras.

En la Unión Europea, el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) se centrará no solo en la seguridad de los datos, sino también en las prácticas de privacidad que van más allá del alcance de otras leyes de notificación de privacidad y violación de información. El reglamento se aplicará a todas las entidades que operan en la UE, así como a aquellas que almacenan o procesan la información de identificación personal de los residentes de la UE, y permite multas de 20 millones de euros o hasta el 4% de la facturación anual, lo que sea mayor. Para las aseguradoras con una exposición significativa en la UE, las multas de GDPR basadas en la facturación global representan una expansión significativa de la exposición cuando se manejan los datos de los clientes.

El riesgo cibernético abarcará de manera inherente múltiples dominios de habilidades funcionales, que requerirán experiencia de reclamos, suscripción, gestión actuarial y de riesgo empresarial, haciendo que el proceso sea verdaderamente un esfuerzo de equipo en una aseguradora. Abordar la brecha de talento mediante la contratación de personas con la experiencia de suscripción cibernética adecuada y la experiencia técnica para evaluar el riesgo y ejecutar estrategias cibernéticas bien definidas será fundamental para la gestión eficaz del riesgo.

Publicado por A.M. Best Rating Services, Inc.

INFORME ESPECIAL

A.M. Best Rating Services, Inc.
Oldwick, NJ
CONSEJERO Y PRESIDENTE **Larry G. Mayewski**
VICE PRESIDENTE EJECUTIVO **Matthew C. Mosher**
DIRECTOR EJECUTIVO **Douglas A. Collett, Edward H. Easop, Stefan W. Holzberger, Andrea Keenan, James F. Snee**

OFICINAS CENTRALES
1 Ambest Road,
Oldwick, NJ 08858
Phone: +1 908 439 2200

CIUDAD DE MÉXICO
Paseo de la Reforma 412,
Piso 23,
Mexico City, Mexico
Phone: +52 55 1102 2720

LONDRES
12 Arthur Street, 6th Floor,
London, UK EC4R 9AB
Phone: +44 0 20 7626 6264

DUBAI*
Office 102, Tower 2,
Currency House, DIFC
P.O. Box 506617,
Dubai, UAE
Teléfono: +971 4375 2780
*Regulado por la DFSA como oficina representativa.

HONG KONG
Unit 4004 Central Plaza,
18 Harbour Road,
Wanchai, Hong Kong
Phone: +852 2827 3400

SINGAPUR
6 Battery Road, #39-04,
Singapore
Phone: +65 6303 5000

Calificación de Fortaleza Financiera de Best (FSR por sus siglas en inglés) es una opinión independiente respecto a la fortaleza financiera y capacidad de cumplimiento ante las obligaciones contractuales y derivadas de la emisión de pólizas vigentes de una aseguradora. Una calificación FSR no es asignada a pólizas u contratos en específico.

Calificación Crediticia de Emisor de Best (ICR por sus siglas en inglés) es una opinión independiente respecto a la capacidad de cumplimiento de una entidad ante sus obligaciones financieras vigentes, puede ser emitida bajo un contexto de corto o largo plazo.

Calificación Crediticia de Deuda de Best (IR por sus siglas en inglés) es una opinión independiente respecto a la calidad crediticia asignada a emisiones, indica la capacidad de cobertura de las condiciones derivadas de la obligación y puede ser emitida bajo un contexto de corto o largo plazo (obligaciones con vencimientos originales menores a un año).

Declaración de Calificación: Uso y Limitantes
Una Calificación de Crédito de Best (BCR; por sus siglas en inglés) es una opinión independiente y objetiva a futuro sobre la relativa capacidad crediticia de un asegurador; emisor u obligación financiera. La opinión representa un exhaustivo análisis que consiste en una evaluación cuantitativa y cualitativa de la fortaleza del balance general, desempeño operativo, perfil del negocio y administración de riesgo integral, o, cuando sea apropiado, sobre la naturaleza específica y los detalles de un instrumento financiero. Debido a que la BCR es una opinión a futuro a partir de la fecha en que se publica, no puede ser considerada como un hecho o garantía de calidad crediticia futura y por ello no puede ser descrita como exacta o inexacta. La BCR es una medida relativa de riesgo que implica la calidad de crédito, y es asignada utilizando una escala con una población definida de categorías y escalones. Las entidades u obligaciones a las que se asigne el mismo símbolo BCR desarrollado con la misma escala, no deberán ser vistas como completamente idénticas en términos de calidad crediticia. En otras palabras, son parecidas en categoría (o escalones dentro de una categoría), pero dado que existe una progresión de categorías prescrita (y de escalones) utilizada en asignar las calificaciones de una población mucho mayor de entidades y obligaciones, las categorías (escalones) no pueden reflejar las sutilezas exactas del riesgo inherente entre entidades u obligaciones calificadas de forma similar. Aunque una BCR refleja la opinión de A.M. Best Company Rating Services Inc. (A.M. Best) sobre la relativa capacidad crediticia, no es indicador o predictor de restricción en el uso de recursos financieros o de probabilidad de incumplimiento definidas con respecto a un asegurador; emisor u obligación financiera específicos. La BCR no es un consejo para invertir y de igual manera no debe interpretarse como servicio de consultoría o asesoramiento, como tal, no están destinados a ser utilizados como una recomendación para adquirir; mantener o concluir una póliza de seguros, contrato, valor o cualquier otra obligación financiera, tampoco señala la idoneidad de cualquier póliza o contrato para un comprador o propósito en específico. Los usuarios de una BCR no deben depender de la misma para tomar una decisión de inversión, sin embargo, si es usado, el BCR debe ser considerado sólo como un factor. Los usuarios deberán hacer su propia evaluación de cada decisión de inversión. Una opinión de BCR es dada bajo las condiciones "actuales" y no cuenta con una garantía expresada o implícita. Adicionalmente, un BCR puede ser cambiado, suspendido o retirado en cualquier momento por cualquier razón a discreción de A.M. Best.

Version 021518