

Comunicado de prensa

Pese a sus complejidades, tanto aseguradoras como empresas pueden afrontar el riesgo cibernético, según un informe *sigma* de Swiss Re: lanzamiento oficial del Swiss Re Institute.

- Los costes potenciales originados por ciberataques están aumentando a gran velocidad; la seguridad y la resiliencia cibernética preocupan cada vez más a las empresas
- Se está desarrollando con rapidez un mercado especializado en ciberseguro, pero el grado de cobertura todavía es relativamente modesto
- Innovaciones de productos y procesos, Big Data y analíticas inteligentes, ayudarán a impulsar soluciones de ciberseguro mejoradas
- Los gobiernos pueden desempeñar un papel importante a la hora de aumentar la resiliencia cibernética
- Este es el primer informe publicado por Swiss Re Institute, que se presenta hoy oficialmente

Zúrich, 1 de marzo de 2017 – El riesgo cibernético es un problema que preocupa cada vez más a las empresas, y recientes ataques han demostrado que los costes de una violación cibernética pueden ir mucho más allá de la gestión de las consecuencias de la pérdida o corrupción de datos. El último informe *sigma* de Swiss Re «Cibernética: cómo enfrentarse a un riesgo complejo», afirma que es necesario que las empresas hagan mucho más para integrar la ciberseguridad en sus programas de gestión de riesgos. Hay en marcha iniciativas para estimular la resiliencia cibernética. Se está desarrollando rápidamente un mercado especializado en ciberseguro, pero hasta ahora el alcance de la cobertura es modesto respecto a la exposición potencial. La innovación de productos y procesos, junto con la analítica avanzada, ayudarán a impulsar soluciones de ciberseguro mejoradas y ampliarán tanto los límites de asegurabilidad como el alcance de cobertura. Finalmente, es posible que algunos riesgos cibernéticos, especialmente los relacionados con eventos de pérdidas catastróficas extremas, no sean asegurables.

Darren Pain, Zúrich
Teléfono +41 43 285 2504


Kurt Karl, Armonk
Teléfono +1 914 828 8686

Jonathan Anchen, Bangalore
Teléfono +91 80 4900 2650

Investor Relations, Zúrich
Teléfono +41 43 285 4444

Swiss Re Ltd
Mythenquai 50/60
Apartado postal
CH-8022 Zúrich

Teléfono +41 43 285 2121
Fax +41 43 285 2999

www.swissre.com
 @SwissRe

Recientes ataques cibernéticos de alta repercusión demuestran que, cada vez más, los costes de una violación de ciberseguridad van más allá de la gestión de los efectos de la pérdida o corrupción de datos. Las empresas ahora deben tener en cuenta los posibles daños a su reputación, daños materiales y propiedad intelectual, y también interrupción de actividades comerciales. El creciente alcance y magnitud de los costes potenciales asociados con ciberincidentes refleja la constante evolución del panorama de riesgo cibernético, que a su vez está siendo conformado por tres dinámicas principales:

- La creciente velocidad y alcance de la transformación digital;
- Las fuentes cada vez más amplias de vulnerabilidad como consecuencia de la hiperconectividad, con la rápida propagación de, por ejemplo, dispositivos con conexión a Internet y computación en la nube;
- Y la cada vez mayor sofisticación de *hackers* que están muy interesados en los posibles beneficios económicos como consecuencia de ciberataques exitosos.

Pese a la mayor concienciación respecto a los peligros, las compañías están por lo general mal preparadas para hacer frente a riesgos cibernéticos. Han sido relativamente pocas las que han integrado la ciberseguridad en su sistema de gestión de riesgos. La regulación podría ser un catalizador para el cambio, ya que en muchas jurisdicciones se está desarrollando legislación que obliga a las compañías a introducir mayores medidas de protección de datos. Como resultado, «las compañías, tanto grandes como pequeñas, deben invertir más en arquitectura de ciberseguridad para desarrollar sólidas capacidades de gestión de riesgos antes y después de pérdidas», afirma Kurt Karl, economista jefe de Swiss Re.

Gestionar un riesgo complejo

Muchas compañías desean transferir riesgos cibernéticos a terceros en mejores condiciones para absorberlos. «Se está desarrollando un mercado específico de ciberseguro y cada vez hay más aseguradoras que desean ampliar el negocio en este ramo especializado », continúa Kurt Karl. El seguro cibernético específico ofrece normalmente protección básica contra violaciones de seguridad de redes y datos y pérdidas asociadas, con límites de capacidad en el mercado que actualmente oscilan entre 5 y 100 millones de USD. Sin embargo, algunos riesgos cibernéticos importantes aún están sin asegurar en gran parte y la escala de cobertura existente es modesta respecto a las exposiciones globales de las compañías.

Una limitación importante para el desarrollo de soluciones de seguro guarda relación con la naturaleza intrínseca de los riesgos cibernéticos. Son complejos y difíciles de cuantificar, especialmente dada la vertiginosa evolución del entorno tecnológico y la carencia de datos de siniestros cibernéticos históricos que servirían para extrapolar información sobre posibles futuras pérdidas. Las aseguradoras y los proveedores de analítica de riesgos están experimentando con diferentes enfoques de modelización del riesgo cibernético, incluyendo análisis determinísticos de escenarios y modelos probabilísticos, en un intento de calcular las posibles pérdidas por eventos cibernéticos. La experiencia de otros peligros, como catástrofes naturales, ofrece la esperanza de que los modelos continúen mejorando a medida que evolucione la comprensión de los factores de riesgo fundamentales y se disponga de más datos sobre pérdidas cibernéticas.

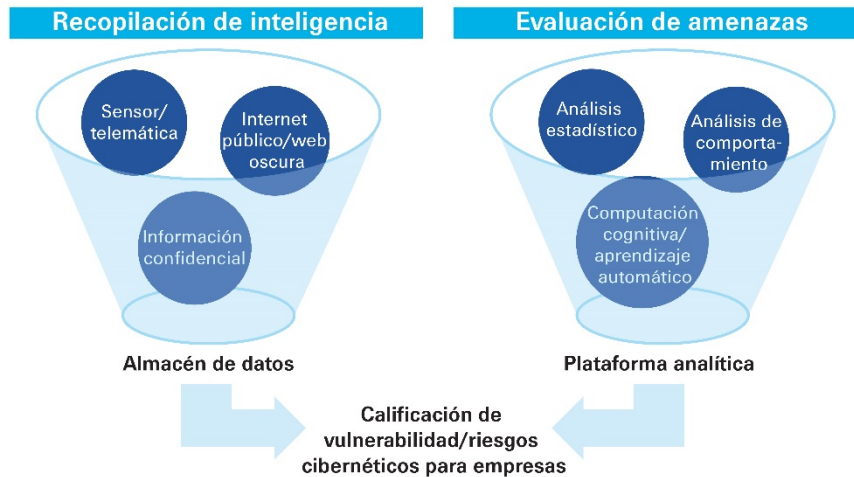
Innovación de productos y procesos

Mientras tanto, la innovación de productos y procesos en el seguro y otros mecanismos de transferencia de riesgos desempeñarán un papel importante a la hora de mejorar las capacidades de gestión de riesgos cibernéticos. Un factor crucial que influirá en el ritmo de la innovación será la obtención y el análisis de la información relevante sobre amenazas y datos que es necesaria para suscribir riesgos cibernéticos con precisión. La industria trabaja constantemente para mejorar la recopilación y divulgación de información. Por ejemplo, varios proveedores de analítica de riesgos han creado programas de datos que proporcionan a las empresas un método estandarizado para identificar, cuantificar e informar sobre exposición cibernética a las aseguradoras¹. De modo similar, el CRO Forum está promoviendo un lenguaje y marco común para las empresas con el fin de obtener información relevante sobre incidentes cibernéticos y vulnerabilidades.

Las aseguradoras, por su parte, tratan de desarrollar productos de seguro menos complejos y más flexibles. Esto incluye coberturas que puedan adaptarse a pequeñas y medianas empresas, que hasta ahora han estado desatendidas por el seguro y frecuentemente están peor situadas para hacer frente a riesgos cibernéticos que las empresas más grandes. Además, algunas re/aseguradoras buscan colaborar con empresas de ciberseguridad y proveedores de analíticas de datos para llenar sus lagunas de conocimiento y ampliar/proporcionar servicios adicionales a sus clientes. En líneas generales, la analítica avanzada puede aumentar las herramientas tradicionales de suscripción de las re/aseguradoras, y ayudarles a responder rápidamente a factores de riesgo subyacentes en rápida evolución.

¹ Véase, por ejemplo, «[RMS Launches New Data Standard for Managing Cyber Insurance](#)», *rms.com*, 19 de enero de 2016, y [Verisk Cyber Exposure Data Standard and Preparer's Guide](#), AIR, 2016.

Figura 1: Analítica inteligente como herramienta de suscripción complementaria



Fuente: Swiss Re Economic Research & Consulting.

Otra forma de incrementar la capacidad de absorción de pérdidas global para el riesgo cibernético es el desarrollo de vehículos de inversión que permitan a los inversores del mercado de capitales asumir algunas de las exposiciones. Actualmente hay en marcha algunas iniciativas para desarrollar valores vinculados al seguro (ILS, por sus siglas en inglés) que cubran riesgo de tipo operativo como el cibernético. El mercado ILS de riesgos cibernéticos está todavía en sus inicios pero podría crecer.

Función de respaldo de los gobiernos

Para ampliar los límites de la asegurabilidad, las empresas deberán trabajar con sus aseguradoras para crear un mercado que sea sostenible. Los gobiernos también tienen una función importante que desempeñar a la hora de promover resiliencia cibernética, incluyendo medidas para mejorar la obtención y difusión de información cibernética y la elaboración de leyes y regulaciones sobre cómo se usa y protege el ciberespacio. Al remodelar incentivos y aumentar la concienciación sobre las ciberamenazas, los gobiernos podrían conducir al sector privado hacia mejores soluciones impulsadas por el mercado. En última instancia, sin embargo, el volumen potencial de pérdidas ocasionadas por algunos eventos cibernéticos podría ser demasiado grande para ser absorbido por el sector privado re/asegurador, especialmente en el caso de eventos de pérdidas máximas como una alteración generalizada de infraestructuras o redes críticas que podría ocasionar significativas pérdidas acumuladas.

Esperamos que haya disfrutado de la lectura de este informe *sigma*, el primero publicado bajo la insignia de «Swiss Re Institute». Swiss Re Institute se presenta formalmente el 1 de marzo de 2017 y tiene como objetivo consolidar la posición de Swiss Re como líder de pensamiento del sector, reuniendo las diversas capacidades de investigación y divulgación de alto nivel de la empresa bajo una misma enseña. Swiss Re Institute elaborará informes de investigación de Swiss Re incluyendo *sigma*, la publicación de investigación líder en el sector asegurador.

Notas a los redactores

Swiss Re

El Grupo Swiss Re es un proveedor líder de reaseguros, seguros y otras formas de transferencia de riesgos basadas en los seguros. El negocio del Grupo tiene lugar tanto de forma directa como también a través de corredores y su base de clientes global incluye aseguradoras, empresas de tamaño medio a grande y clientes del sector público. Swiss Re ofrece desde productos estándar hasta coberturas a la medida en todos los ramos del negocio y despliega la fortaleza de su capital, sus conocimientos especializados y sus innovaciones para contribuir a que sea posible asumir los riesgos, algo de lo que dependen las empresas y el progreso de la sociedad en general. Fundada en Zúrich, Suiza, en 1863, Swiss Re sirve a sus clientes a través de una red de más de 70 oficinas en todo el mundo y ha recibido la calificación «AA-» de Standard & Poor's, «Aa3» de Moody's y «A+» de A.M. Best. Las acciones nominativas del Grupo Swiss Re que posee la sociedad tenedora, Swiss Re Ltd, se cotizan en la bolsa suiza SIX de acuerdo con el International Reporting Standard y se negocian bajo el símbolo SREN. Si desea más información sobre el Grupo Swiss Re, visite www.swissre.com o siganos en Twitter @SwissRe.

Cómo solicitar el envío del estudio *sigma*:

Las versiones electrónicas en inglés, alemán, francés y español del estudio *sigma* N.º 1/2017, *Cibernética: cómo enfrentarse a un riesgo complejo* están disponibles en el servidor de Swiss Re: www.swissre.com/sigma.

Las ediciones impresas de *sigma* N.º 1/2017 en inglés, francés, alemán y español ya están disponibles. Las versiones impresas en chino y japonés estarán disponibles en breve. Envíe su solicitud, indicando su dirección postal completa, a sigma@swissre.com.