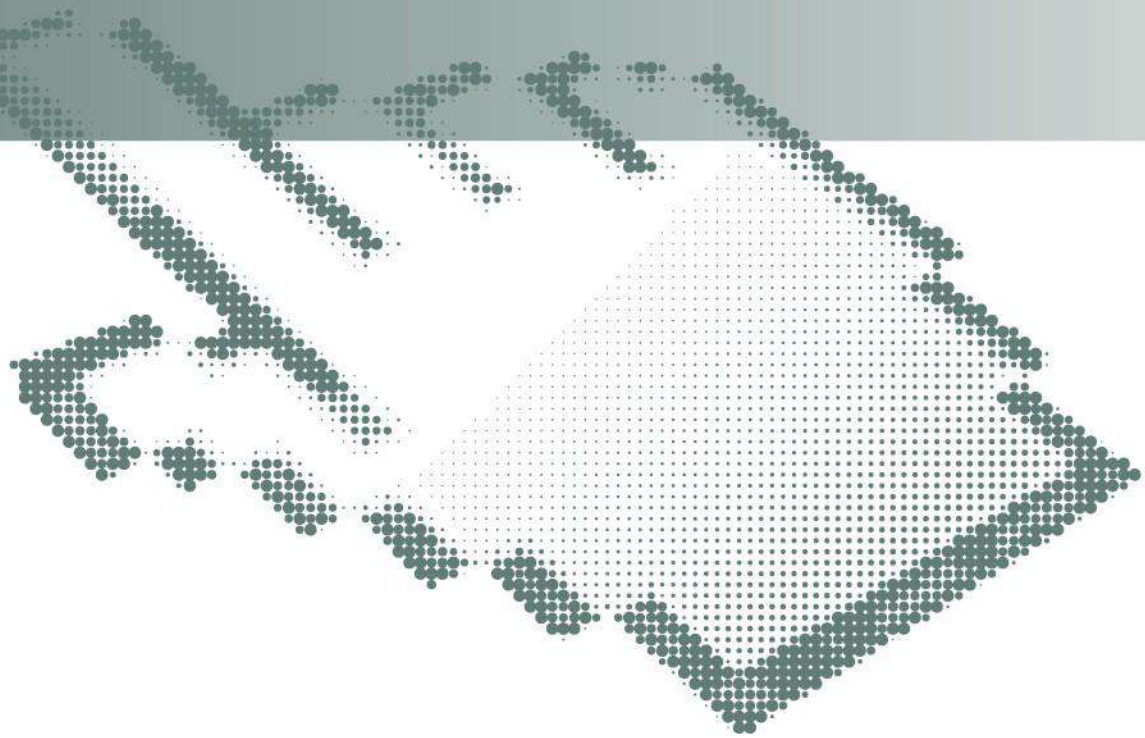
Swiss Re

Introducción al Riesgo Cibernético

BISA, Noviembre 2017



Índice/Programa

- Introducción al seguro cibernético
- Cobertura contra riesgo cibernético en otros tipos de pólizas de seguro de responsabilidad civil
- Mercado de seguro cibernético
- Siniestros
- Acumulación y reaseguro

Introducción al seguro cibernético

Riesgo cibernético

Activo de información	• Datos de valor financiero que son procesados, almacenados o transmitidos mediante una computadora
Amenaza	• Algo que podría causar daños a un sistema o una organización.
Vulnerabilidad	• Una falla o debilidad que puede usarse para atacar a un sistema o una organización
Controles	• Procedimiento o política que proporciona seguridad razonable de que la tecnología de la información opera como está previsto, de que los datos son confiables y de que la organización cumple con las leyes y regulaciones aplicables.

Seguro cibernético: ¿qué cubre?

Ofrecemos cobertura para...

primera parte

- Interrupción del negocio (BI) e interrupción del negocio contingente
- Restauración de datos
- Ciberextorsión
- Delitos informáticos

terceros

- Defensa regulatoria
- Costos de respuesta ante incidentes (incluida notificación, investigación forense, PR, seguimiento)
- Responsabilidad en medios de comunicación
- Responsabilidad de redes y seguridad informática

Exclusiones estándares

- Defraudación de patentes y apropiación indebida de secretos comerciales
- Cobertura de primera parte por daños a la propiedad intelectual
- Daños de marca y de reputación
- Cobertura exclusiva por interrupción del negocio contingente (CBI)
- Cobertura independiente por extorsión
- Guerra cibernética

Gestión y evaluación de riesgos cibernéticos

- Revisión independiente
- Información crítica
- Respuesta oportuna al ataque cibernético
- Sensibilización y formación
- Adaptación periódica

Cobertura contra riesgo cibernético en otros tipos de pólizas de seguro de responsabilidad civil

Indemnización profesional (errores y omisiones)

Cubre pérdidas financieras resultantes de un acto, un error o una omisión en la prestación de servicios profesionales.

Históricamente, las pólizas de indemnización profesional no incluían cobertura para exposiciones cibernéticas. Algunas profesiones (p. ej. médicos, abogados y contadores) tienen un mayor deber de protección respecto a la información y a los datos personales de sus clientes.

Ejemplo: si se produce una violación de datos en un estudio jurídico y se roba información sensible de un cliente, los abogados posiblemente se consideren responsables y su póliza de indemnización profesional cubriría la pérdida.

Algunas aseguradoras de responsabilidad profesional están comenzando a incorporar cláusulas adicionales con sublímites para tratar de determinar la cobertura de manera proactiva. En algunos casos, ofrecen incluso un límite para coberturas de primera parte (es decir, gasto de notificación, restauración de datos, interrupción del negocio).

Las aseguradoras de responsabilidad profesional de médicos y hospitales están comenzando a excluir las exposiciones a riesgos cibernéticos debido a la naturaleza sensible de las leyes en EE.UU. respecto de la protección de registros médicos. Estos médicos y hospitales están entonces obligados a proporcionar cobertura independiente contra riesgo cibernético.

Responsabilidad de Directores y Ejecutivos (D&O)

Cubre siniestros por pérdidas financieras originadas en actos del directorio o de la dirección en su carácter de directores o ejecutivos.

Históricamente, las pólizas de D&O no incluían cobertura contra riesgo cibernético.

A modo de ejemplo, si se produce una violación de datos en una empresa y esto provoca una importante pérdida financiera y una caída de la cotización de las acciones, los accionistas pueden demandar a los directores y ejecutivos por no haber cumplido con el deber de proteger los activos de la empresa.

Los accionistas han intentado iniciar tales acciones en muchas ocasiones — un caso resonante fue el de Target (empresa de productos masivos) / violacion de datos —, las cuales no han prosperado hasta la fecha. Sin embargo, los abogados de los demandantes continúan iniciando acciones al amparo de pólizas D&O (los casos más recientes, Wendy's y Yahoo!), de modo que no me sorprendería que lograran su objetivo en un futuro no muy lejano.

Siniestros cibernéticos y consiguientes lesiones físicas o daños materiales

Cubre al asegurado por las sumas de dinero que la ley le obliga a pagar como consecuencia de lesiones físicas o daños materiales.

Las pólizas de responsabilidad general excluyen la responsabilidad por pérdida o robo de datos electrónicos. La Oficina de Servicios de Seguro (ISO), principal responsable de la redacción de pólizas de responsabilidad general, introdujo cláusulas adicionales en 2014 que excluyen siniestros derivados del acceso o la divulgación de información confidencial o personal, pero permite reducciones salariales en caso de lesiones físicas.

Ejemplo: un pirata informático obtiene acceso a una plataforma petrolera, provoca intencionalmente la explosión de un pozo e importantes lesiones físicas, y daños materiales y ambientales. O bien, un pirata informático obtiene acceso a los controles electrónicos de un tren y provoca un gran accidente ferroviario.

Las pólizas tradicionales de seguro cibernético no ofrecen cobertura por lesiones físicas o daños materiales provocados por una pérdida o la mala utilización de datos electrónicos, de modo que esta pérdida, en teoría, estaría cubierta por la póliza de responsabilidad general del asegurado. Algunas aseguradoras de riesgo cibernético están comenzando a ofrecer esa cobertura.

Hasta el momento, no se ha registrado un siniestro cibernético con importantes daños materiales o lesiones físicas, y las aseguradoras de responsabilidad general normalmente no consideran esta exposición al asumir los riesgos de suscripción.

Mercado de seguro cibernético

El mercado estadounidense es el mayor mercado de seguro contra riesgo cibernético con una marcada orientación hacia la privacidad de los datos personales.

Primas brutas suscritas por USD 2000-2500 millones

Tasas de crecimiento del 25% al 30% en los últimos 10 años

'...EE. UU. ha sido el primer mercado en adoptar productos independientes de seguro cibernético con soluciones centradas en torno a la violación de datos. Las aseguradoras prevén que habrá un mayor interés de otros países puesto que la reglamentación y una mayor conciencia sobre el tema impulsan la demanda.'[1]

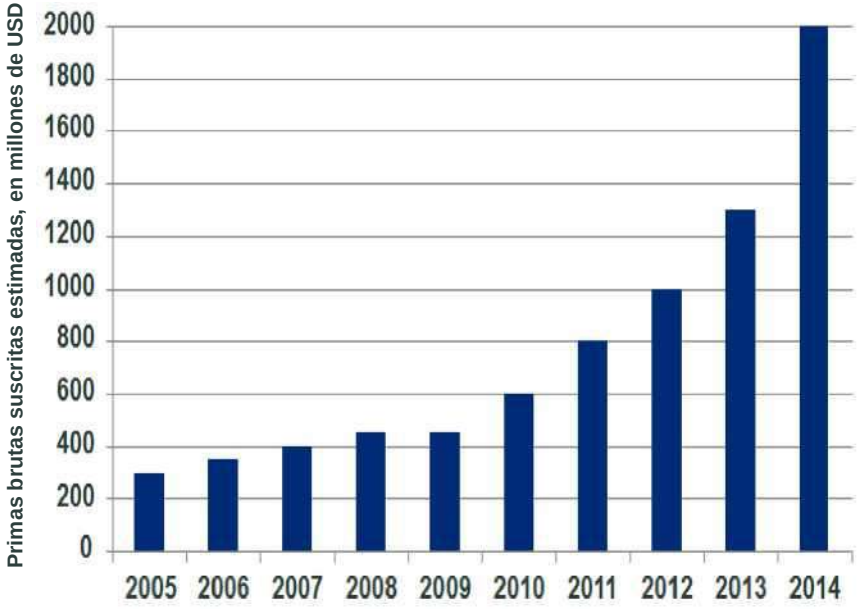
El principal catalizador del crecimiento y tamaño que tiene actualmente el mercado estadounidense fue la sanción de leyes sobre notificación de fallas en la seguridad de los datos (que fuera aplicada por primera vez en California en 2002), lo que aumentó la demanda de cobertura para violaciones de datos. Hoy, 48 de los 50 estados tienen leyes sobre notificación de fallas en la seguridad de los datos. Las tasas de penetración del seguro cibernético parecen estar muy correlacionadas con la aplicación de las respectivas reglamentaciones [2]

Se prevé que el mercado de seguro cibernético en EE.UU. alcance un valor de USD 8000-10.000 millones para 2025, lo que representa alrededor del 3% del mercado total estadounidense.

1 S&P, Looking Before They Leap: U.S. Insurers Dip Their Toes In The Cyber-Risk Pool
2 Advisen, Cyber Risk Insights Conference (Congreso sobre Riesgos Cibernéticos)

El mercado de seguro cibernético en EE.UU. registró un crecimiento casi exponencial en los últimos 10 años.

Crecimiento de las primas de seguro cibernético en EE.UU.



Fuente: The Betterley Report, informes sobre estudios del mercado de seguro contra riesgos cibernéticos/de privacidad

Prima bruta suscrita estimada en EE.UU., en millones de USD

Se espera que continúe creciendo debido a una mayor toma de conciencia entre las empresas y corporaciones, las condiciones y la evolución del marco regulatorio, y a una digitalización cada vez mayor de la economía.

Fuente 1 The Betterley Report, informes sobre estudios de mercado de seguro de privacidad/contra riesgos cibernéticos
Fuente2 http://www.scmagazineuk.com/aig-cyber-insurance-sales-have-risen-by-30/article/329623

El mercado europeo tiene un tamaño menor al de EE.UU. y está mucho más orientado a coberturas de primera parte.

Primas brutas suscritas por aproximadamente USD 300 millones
Sólido crecimiento

'..."Fuera de EE.UU., el seguro contra riesgos cibernéticos no ha concitado gran atención, [...] pero la reglamentación sobre protección de datos en Europa y en el resto del mundo habrá de modificar esta realidad."[1]

En general, el mercado europeo se caracteriza por un mayor énfasis en las coberturas de primera parte y, en general, por un mayor tamaño de las líneas.
Las tasas de contratación y la penetración del mercado aún son débiles y el mercado parece estar expectante. El ciclo de contratación de las coberturas de seguro (a menudo para quienes contratan por primera vez) suele ser largo.
Muchas compañías aseguradoras más pequeñas están desarrollando actualmente su propia oferta de seguro cibernético.

"Según estimaciones, el mercado europeo tendrá un tamaño de entre EUR 700 millones y EUR 900 millones para el año 2018. El proyecto de normas sobre protección de datos de la UE podría dar un fuerte impulso al mercado europeo de seguro cibernético..."[2]

1 Marsh: UK Cyber Security, The Role of Insurance in Managing and Mitigating the Risk
2 GuyCarpenter: Ahead of the Curve: Understanding Emerging Risks 9/2014

El mercado asiático de seguro cibernético aún es muy incipiente

Primas brutas suscritas por aproximadamente USD 200 millones
Se prevé un sólido crecimiento

'En los últimos tres años, en AIG Singapur se han septuplicado las consultas sobre pólizas de seguro cibernético.'[1]

Según una encuesta realizada por la Conferencia de Reaseguro Internacional de Singapur (SIRC) en noviembre de 2015, el 40% de los encuestados actualmente están desarrollando nuevas coberturas contra riegos cibernéticos, pero el 43% expresó que aún no habían comercializado ninguna póliza.

Se prevé que el mercado asiático de seguro cibernético crezca a alrededor de mil millones en los próximos 3 a 4 años.

AIG China espera que la demanda de seguro cibernético aumente considerablemente tras el reciente ataque del malware "WannaCry".[2]

1 CIO Asia, 31 de marzo de 2016
2 Reuters, 9 de agosto de 2017

Observaciones del mercado de seguro cibernético

- El panorama del riesgo cibernético está en continua evolución
- La armonización de la reglamentación y las tendencias tecnológicas tienen un fuerte impacto en el riesgo y en el mercado de seguro.
- El mercado cibernético de EE.UU. es el más desarrollado. Si bien los mercados de Europa y Asia siguen siendo pequeños en tamaño, se espera un enorme crecimiento en los próximos años.
- La reglamentación es clave en el desarrollo del mercado.
- Según la región, las empresas tienen una percepción diferente del riesgo cibernético del asegurado directo y a terceros.

Oportunidad:
Las empresas (aún) no contratan seguro cibernético porque aún no han estudiado las coberturas o porque consideran que no están expuestas a riesgos cibernéticos.

Siniestros

Fallas de seguridad en los datos

110M de registros personales robados

109M de registros personales robados

32M de registros personales robados

153M de cuentas violadas

100 terabytes de datos

80M de registros de salud

IDENTITY THEFT RESOURCE CENTER

Periodo: 2005 - 2017

Cantidad de violaciones = 7630

Cantidad de registros = 898.775.527

Interrupción del negocio

- A las 13:09 horas, el 20 de julio de 2016, un router del centro de datos de Southwest Airlines en Love Field tuvo una falla de seguridad, lo que creó un punto crítico que paralizó cientos de las aplicaciones de software de la empresa.
- En total, la aerolínea canceló alrededor de 2300 vuelos entre miércoles y domingo. Eso representa alrededor del 11% de los 19.500 vuelos que el operador manejaba en ese lapso de tiempo.

(Fuente: Dallas News)

- El 27 de marzo, un grave fallo informático hizo caer las redes de British Airways, lo que afectó a sus principales centros de Heathrow y Gatwick en Londres.
- Un ingeniero había desconectado la fuente de alimentación en el centro de datos cerca del aeropuerto de Heathrow en Londres, lo que causó una sobretensión que generó grandes daños al reconectarse.
- La aerolínea con base en Reino Unido se vio obligada a cancelar miles de vuelos durante el ajetreado fin de semana de feriado bancario.
- Se cancelaron más de 1000 vuelos y 75.000 pasajeros resultaron afectados por esta falla. Según estimaciones de los analistas, el hecho le costará más de 100 millones de libras a la aerolínea.

(Fuente: Forbes)

WannaCry

El malware afectó a más de 200.000 computadoras en 150 países en mayo de 2017. Las áreas más afectadas fueron Rusia, Ucrania, India y Taiwán.

Esto afectó esencialmente a pequeñas y medianas empresas europeas y asiáticas, que anteriormente no contaban con cobertura de seguro cibernético, de modo que esto no constituyó una gran pérdida para la industria del seguro en general.

El malware está en continua evolución, de modo que es solo cuestión de tiempo hasta que un virus similar provoque pérdidas catastróficas a empresas de todo el mundo, incluidas las compañías de seguro.

Acumulación y reaseguro

Los tres riesgos principales de agregación según Swiss Re

DoS/IO

(Denegación de servicio/interrupción del negocio)

- Ejemplo 1: Ataque coordinado que hace caer muchos portales de ventas en línea
- Ejemplo 2: Ataques a la nube o a una nube de nubes
- Ejemplo 3: Interrupción del servicio de Internet a gran escala

Cobertura afirmativa: afecta principalmente a productos cibernéticos especializados

Violación de datos

(Impacto sobre los datos personales o financieros)

- Datos personales o información de tarjeta de crédito robada de un sistema de base de datos ampliamente usado

Cobertura afirmativa: afecta principalmente a productos cibernéticos especializados

Infraestructura crítica

(con o sin daños materiales)

- Un virus bloquea el sistema de refrigeración de varias plantas eléctricas, lo que inicia explosión/incendio
- A raíz del malware, se cae la transmisión eléctrica sin daños materiales

Cobertura "silenciosa" incorporada en productos estándares

¿Desea obtener más información?

Publicaciones de Swiss Re

sigma **n.° 1/2017**

Según afirma Swiss Re *sigma*, a pesar de sus complejidades, las aseguradoras y empresas pueden hacer frente al riesgo cibernético; lanzamiento oficial Swiss Re Institute

Las amenazas cibernéticas están evolucionando con rapidez debido a la creciente digitalización de la sociedad, la utilización generalizada de dispositivos y procesos por Internet, y el perfil cambiante de los hackers. Los recientes ataques cibernéticos de alto perfil demuestran que la magnitud de las posibles pérdidas asociadas también se está ampliando, para cubrir cada vez más daños financieros y físicos relacionados con la violación a la privacidad de los datos y con los activos tangibles e intangibles de las empresas,como así también con los costos de la interrupción del negocio. En consecuencia, el tema de la protección cibernética comienza a ocupar un lugar más preponderante en la agenda de las empresas, tanto grandes como pequeñas.

RESPONSABILIDAD CIBERNÉTICA: VIOLACIÓN DE DATOS EN EUROPA

8 de marzo de 2017

Esta publicación escrita por Elena Jelmini Cellerini y Christian Lang analiza las consecuencias de una violación de datos en Europa, y compara las situaciones en Europa y EE. UU. en lo que se refiere a las principales características de tal hecho. Describe en qué punto se encuentra el debate a principios de 2017, casi 18 meses antes de que entre en vigencia la nueva Normativa Europea de Protección General de Datos. Un indicador que también permite dar una idea de hacia dónde parece dirigirse Europa consiste en analizar la jurisprudencia en gestación, en especial en el Reino Unido, donde se han tomado algunas decisiones emblemáticas. El Reino Unido tiene previsto implementar esta normativa pese a su salida de la Unión Europea.