DEL CIBERRIESGO AL CIBERSEGURO

Crece la oferta de seguros Cyber en la Argentina

Los ciberataques masivos mundialmente famosos impulsan legislaciones cada vez más estrictas sobre la gestión de datos personales. Estos marcos normativos, a su vez, son la plataforma para el despegue de los seguros cibernéticos. En nuestro país ya hay cuatro aseguradoras que ofrecen coberturas al segmento corporativo y pyme. Todas tienen foco en responsabilidad civil, daños propios y gestión de crisis. Los ataques ransomware que secuestran datos crecen sin control y las pólizas incluyen reembolsos por pagos de rescates.

El robo de datos, el fraude digital y los ciberataques son los principales riesgos

El Informe Global de Riesgos 2019 del *Foro Económico Mundial*, realizado junto a *Marsh & McLennan Companies*, señala que el robo de datos, el fraude digital y los ciberataques son los principales riesgos por probabilidad para este año. Y los empresarios lo saben. Según el *Allianz Risk Barometer 2019*, elaborado por *Allianz Global Corporate & Specialty*, los ciberriesgos están primeros (junto a la interrupción del negocio) en el ranking de los riesgos más temidos por las empresas a nivel mundial, índice del que participaron 2.415 expertos de 86 países.

Teniendo en cuenta que el 94%

de la documentación comercial del mundo es digital, es bien obvia la preocupación. Todo abona a la imagen de la propagación de los virus informáticos al mejor estilo *apocalipsis zombie*.

EMERGENTE. Sin embargo, desde la óptica del risk management y de la industria aseguradora, el ciberriesgo califica de *emergente*. No es que los hackers sean algo nuevo, sino que el terreno sobre el que trabajan es cada vez más fértil y el daño que pueden hacer va tomando dimensiones cinematográficas.

Martín Elizalde, abogado especialista en seguridad informática y partner de *Foresenics*, entiende que, de los riesgos a cubrir por la industria de seguros, el cibernético es el más importante. "Nada es comparable al riesgo informático, por la magnitud, la amplitud y la dispersión de los daños y las víctimas. Es muy difícil predecir, su escala puede ser catastrófica y tiene una falta total de direccionalidad y de lógica", indica el especialista que asesora a las aseguradoras para la confección de este tipo de coberturas.

Alcides Ricardes, CEO de *ReSolutions*, una empresa de *RiskGroup Argentina*, sostiene que el mercado internacional tiene a disposición un producto sólido para los hechos de violación de la seguridad y/o de la privacidad: "Cubre dos grandes frentes: por un lado, la responsabilidad civil hacia terceros y, por el otro, el daño material propio, aspecto que tiende a cubrir los gastos de remediación para volver a la situación anterior de seguridad y privacidad". Este directivo remarca que la cobertura disponible es compleja y amplia y que puede cubrir hasta el lucro cesante.

Para los especialistas hoy hay un buen producto con una prima adecuada, pero estiman que, a medida que se vaya desarrollando la siniestralidad, es esperable que las coberturas se empiecen a restringir y que las primas aumenten. "El momento para entrar es hoy", remarca Ricardes. *ReSolutions* hoy trabaja un producto de reaseguro con enfoques diferentes para pymes y grandes empresas.

■ **Elizalde: "En la Argentina durante 2017, nosotros llegamos a atender 11 casos de *ransomware* en un mes. Hay infinidad de ataques de este tipo".**

Matías Ferrari, Facultative Senior Broker del bróker de reaseguros *Special Division*, observa el mismo escenario: "A nivel internacional, hace diez años que se habla de Cyber y las coberturas disponibles son sólidas. Hoy, por el desarrollo que alcanzaron, los reaseguradores están armando Departamentos específicos de Cyber". Ferrari recuerda la primera vez que cotizó este seguro: fue en 2011, en forma facultativa y con el *Lloyds*. "En aquel momento, por una cuestión de costos, resultó invendible en Latinoamérica. Ahora los límites y las primas se acomodaron a la realidad de esta región y a la de las distintas empresas. Incluso hoy los reaseguradores nos proponen ofrecer Cyber como adicional de otras coberturas, para penetrar con este seguro en el mercado", agrega.

El Informe Global de Riesgos 2019 del Foro Económico Mundial señala que el robo de datos, el fraude digital y los ciberataques son los principales riesgos por probabilidad para este año.

MOTOR. El desarrollo de esta cobertura está directamente relacionado con la legislación. "En los países en los que estos seguros fueron ganando terreno, el factor que motorizó las ventas fue la normativa que obliga a las empresas, por un lado, a preservar la información y tener controles adecuados y, por el otro, a reportar las violaciones de seguridad que puedan afectar datos de terceros", señala Ricardes.

El pionero fue Estados Unidos, país que comenzó a imponer a las empresas cargas preventivas, pero también reactivas muy onerosas. Cada Estado le da un tratamiento diferente, pero en general ante un evento de esta naturaleza las empresas tienen que notificar a cada damnificado que su información se vio comprometida por una fuga de datos. Además, deben hacer un monitoreo del crédito y, por ejemplo, garantizar que a esas personas no les suplanten la identidad. El costo de estas acciones post ataque es altísimo multiplicado por la cantidad de terceros afectados en cada caso.

Valga un ejemplo para dimensionar. La central de reservas de *Ma-*

rriott, la mayor cadena hotelera del mundo, fue hackeada el año pasado y los datos (número de pasaporte incluido) de 500 millones de huéspedes quedaron expuestos. *Marriott* debió comunicar el ataque a la comunidad, notificar a cada damnificado y, además, ofrecer a sus clientes en los Estados Unidos una suscripción de un año a un servicio de detección de fraudes.

"En América Latina, en cambio, las legislaciones son más preventivas que reactivas. En la Argentina, por ejemplo, no es obligatorio reportar los ataques cibernéticos. Por eso, si bien hay muchos episodios, no los conocemos", señala Paulina Vélez Gómez, Cyber Broker de Latin America & Caribbean de *Marsh*.

GDPR Y UN CAMBIO DE PARADIGMA. El 25 de mayo de 2018, la Comunidad Europea puso en vigencia un nuevo y estricto Reglamento General de Protección de Datos Personales (GDPR por sus siglas en inglés) que tiene la intención de reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea (UE). También se ocupa de la exportación de datos personales fuera de esa región. Tiene un enfoque muy preventivo y también reactivo: prevé multas de hasta el 4% de la facturación anual de las empresas.

> **"El factor que motorizó las ventas fue la normativa que obliga a las empresas a preservar la información** y a reportar las violaciones de seguridad que puedan afectar datos de terceros."
>
> ***(Ricardes)***

Eventos *bomba* como el robo de información crediticia más importante de la historia fueron impulsores de este endurecimiento de normas: recordemos que los datos de 147 millones de ciudadanos de los EE.UU., Canadá y Reino Unido fueron filtrados mediante un hackeo a *Equifax*, una de las mayores agencias que realiza análisis crediticios (y que está a cargo del *Veraz* en la Argentina).

"Estas exigencias se irán extendiendo cada vez más y con el tiempo las empresas de todo el mundo tenderán a manejarse con los mismos estándares de seguridad", prevé el CEO de *ReSolutions*. En la misma línea opina Roberto Heker, socio de *NextVision*, empresa de ciberseguridad con más de 28 años en el mercado tecnológico. Según Heker, que es, además, cofundador y CEO de *NextVision Iberia*: "Esta normativa elevará los estándares de seguridad a nivel mundial". Este experto señala: "En la Argentina, de hecho, se estudia una actualización de la vigente ley de Protección de Datos Personales 25.326".

Con la cancha marcada por este factor motorizante, la estimación es que el volumen de mercado para el seguro cibernético aumente a US$ 8 o 9 mil millones para 2020.

■ **Heker: "Ante un secuestro, no tenés garantías de que luego del pago procedan a devolverte la información completa, sana y sin quedarse con copias. No lo recomiendo".**

SECUESTRO ONLINE. Los especialistas consultados por **Estrategas** coinciden en que otro factor que motoriza la demanda de coberturas son los ataques masivos que se visibilizan, como el famoso *WannaCry*. El 12 de mayo de 2017, este *ransomware* afectó a más de 230 mil computadores de más 150 países. Durante un ataque de este tipo los datos de las víctimas son encriptados y se solicita un *rescate* económico –pagado con la criptomoneda Bitcoin– para permitir de nuevo el acceso a los mismos. El servicio nacional de salud de Gran Bretaña (NHS), *Telefónica* de España, *FedEx*, la empresa ferroviaria alemana *Deutsche Bahn* y las aerolíneas *LATAM* fueron algunas de las empresas más afectadas por *WannaCry*.

Los perpetradores de estos ataques en general piden rescates de entre US$ 200 y 500 por usuario y en aquella oportunidad logran recaudar un total US$ 140 mil, nada comprado con los millones en daños que ocasionaron.

¿Cuántas personas vieron vulnerada su intimidad con *WannaCry*? No se sabe. Y esa es una preocupación latente para las aseguradoras: es potencialmente infinita la cantidad de demandas que pueden surgir tras eventos como éste. Si hay damnificados, habrá juicios, y si hay juicios habrá abogados que tal vez se interesen en explotar este nuevo nicho. ¿Habría lugar para una industria del juicio en este negocio emergente? "Por ahora es un tema desconocido incluso para los damnificados que no se enteran que sus datos fueron vulnerados, o que no saben que pueden demandar a la empresa que los expuso. Hay que ver cómo evoluciona a medida que vaya creciendo la concienciа sobre esto en la población", anticipa Ferrari.

En principio se puede decir que la siniestralidad no está desarrollada aún, pero hay que tomar nota de los pronósticos: un reporte de ciberseguridad de *Cisco* indica que los ataques de *ransomware* están creciendo a una tasa anual del 350%. "En la Argentina durante 2017, nosotros llegamos a atender 11 casos de *ransomware* en un mes. Hay infinidad de ataques de este ti-

■ **Ferrari: "Hoy los reaseguradores nos proponen ofrecer Cyber como adicional de otras coberturas, para penetrar con este seguro en el mercado".**