CIBERRIESGOS, el hermano mayor del seguro de Protección de datos

El seguro de Ciberriesgos se ha convertido en el hermano mayor de la póliza de Protección de Datos porque cubre lo mismo y además complementa a los productos de Daños, de RC, de D&O, de Pérdida de beneficios, de Infidelidad de empleados... En este tipo de seguros, el servicio que se recibe es tanto o más importante que la indemnización a la que se accede tras un siniestro ciber. Todo eso lo convierte en un producto imprescindible para cualquier empresa y que, en los próximos años, tendrá un gran desarrollo en su contratación.

Luis Moroño.

Macarena Bandrés.

Javier Ybarra.

Carlos Rodríguez.

España es el tercer país del mundo donde más incidentes de seguridad se producen, superando los 200.000 al día. Sin embargo, este mercado potencial no tiene su correspondencia en el mundo asegurador porque, por el momento, el seguro de Ciberriesgos no está desarrollado por muchas aseguradoras. Aunque cada vez hay más productos, según Luis Moroño, director en Inerzia Asesores Correduría de Seguros, "muchos de ellos no se adaptan a lo que es un seguro de Ciberriesgos. Hay productos de compañías generalistas que están aprovechando la inercia de cobertura de pólizas de Hogar en equipos informáticos y recuperación de información y lo están vendiendo como seguro de Ciberriesgos y no lo son. Te encuentras con mucha duplicidad de coberturas y, en algunas ocasiones, cosas tan sorprendentes como que ofrecen el forense informático solo en horario laborable. Eso no es una plataforma de gestión de crisis".

Lo bueno, en opinión de Macarena Bandrés, gerente de cuentas de Reaseguros & Wholesale de Howden, es que "se está haciendo mucha campaña de concienciación entre compañías y corredores para intentar fomentar la importancia que tiene el mensaje".

Javier Ybarra, director de Líneas Financiera para España y Portugal de Chubb, afirma que, "desde nuestra perspectiva de entidad, la venta del seguro de Ciberriesgos está tomando velocidad. Hay un proceso de comprender el riesgo y el corredor tiene un papel fundamental para hacer entender qué ocurre y cómo ocurre. Para vender este producto se necesita la especialización. No puedes entrar si no has hecho un análisis previo y has visto cómo puedes dar respuesta. Es un seguro en el que la respuesta es inmediata, desde el primer día".

Carlos Rodríguez, CyberEdge Product Leader de AIG, coincide en la necesidad de que el broker conciencie a las empresas de que es preciso este producto "y cómo se pueden proteger gracias a un seguro. Hay que explicar que no se trata solo de un problema de sistemas, sino que también tiene una serie de implicaciones legales, financieras y reputacionales que cubre el seguro de Ciberriesgo. Desde hace 4 años que se comenzó a vender este tipo de pólizas en España, puedo decir que el condicionado ha ido evolucionando muchísimo. Estamos adaptando el seguro a las necesidades que nos trasladan los corredores y los clientes y creo que en dos años se incrementará de forma importante la venta de este producto".

Buena catalogación de los ataques

Quizás porque España está recibiendo tantos ataques cibernéticos, nos encontramos entre los 3 países del mundo donde mejor se detectan y se catalogan todas estas incidencias. Luis Moroño comenta que, "en ese sentido, se está haciendo muy bien. Conozco despachos de abogados que dan cursos de ciberdelincuencia y la policía también está haciendo mucho en cuanto a la concienciación".

Algo en lo que está de acuerdo Carlos Rodríguez: "Organismos como Incibe está haciendo una labor fantástica de formación y concienciación en el ámbito privado. Sin embargo, en los siniestros de pymes en los que AIG está involucrada, nos damos cuenta de que

el nivel de madurez de las empresas es bajo cuando el forense solicita información". En este sentido, Macarena Bandrés opina que "es como la D&O que todavía se tiene que adaptar un poco a lo que es el sector pyme".

En el tema de la concienciación, Bandrés señala que "depende del tipo de empresa. Por ejemplo en las industriales sí que tienen mayor concienciación y sí que tienen el producto porque están preocupadas por sus daños propios. Pero en las pymes hay más preocupación por los daños a terceros que puedan causar".

Por eso, el director de Líneas Financiera para España y Portugal de Chubb plantea "acercarse a las pymes por la cobertura de los daños a terceros para después cubrir también los daños propios".

La gerente de cuentas de Reaseguros & Wholesale de Howden insiste en que "para las pymes hay que hacer un producto que sea claro y económico porque muchas de ellas te cuestionan si no tienen cubierto lo mismo en su póliza de Daños".

"Para las pymes hay que hacer un producto que sea claro y económico porque muchas de ellas te cuestionan si no tienen cubierto lo mismo en su póliza de Daños".
Macarena Bandrés

Un producto que necesita especialización

Los participantes en la mesa redonda organizada por PymeSeguros están de acuerdo en que se trata de un seguro para entidades especializadas. Javier Ybarra explica que "la diferencia entre el asegurador especialista y el generalista es la capacidad de dar respuesta a esa preocupación. Primero presentando un producto que tenga un lenguaje claro, evitando tecnicismos o legalismos. Luego, teniendo una capacidad de respuesta desde el primer minuto. No es solo una cobertura de responsabilidad de un daño a un tercero, sino que hay que dar una respuesta, una gestión e incluso una reparación a futuro (en la parte reputacional). El producto ha evolucionado y se ha buscado complementar la póliza de Daños, de RC o de D&O".

Luis Moroño indica que "el valor añadido de esta póliza, sobre todo para una pyme, es el panel de primera respuesta que da acceso a una información o a una serie de servicios que de otra forma no podría tener. Independientemente de los límites y de la indemnización, cuando hay un incidente, la pyme puede llamar y derivar la gestión del asunto a las aseguradoras especialistas".

Carlos Rodríguez añade que "las pymes son objetivos claros porque son más vulnerables ya que no invierten tanto en seguridad y para los cibercriminales es mucho más sencillo el ataque. Por eso, es tan importante poder acceder a ese panel de primera respuesta que la orienta sobre lo que tiene que hacer. Además, suelen ser la puerta trasera de acceso o back door para atacar a grandes compañías con las implicaciones de responsabilidad adquiridas como proveedor. Tampoco hay que olvidar otro asunto vital para las pymes como es la pérdida de beneficios que ocasionan estos ataques. Las pequeñas empresas carecen de planes de contingencia o respuesta de incidentes cibernéticos al considerarlos innecesarios y de alto coste. Por eso, la pérdida de beneficios así como la incapacidad de asumir los costes operativos de una interrupción de negocio, debido a un fallo de seguridad, puede resultar devastadora. La Alianza para la Ciberseguridad de EUU afirma que el 60% de las pymes no pueden seguir abiertas en los seis meses posteriores a recibir un ataque cibernético".

La especialización también se lleva a los corredores. Moroño asegura que "hay muchos brokers que no se atreven a vender Ciberriesgos porque tienen un desconocimiento importante sobre él. No se sienten seguros a la hora de poder vender ese producto". En este sentido, Ybarra comenta que "la póliza de Ciberriesgos necesita un poco de dedicación para saber de qué se está hablando". Por eso, las aseguradoras cada vez dan más información y organizan más actos de divulgación de este producto. Además, como señala Macarena Bandrés, "en los casos más difíciles, nos apoyamos en la aseguradora y vamos con ella a visitar al cliente".

El servicio es fundamental

Se trata de una póliza en la que el servicio que se recibe es tanto o más importante que la indemnización a la que se accede

tras un siniestro de este tipo. Por ejemplo, como dice Ybarra, "en el caso de un riesgo de ciberextorsión es crítico tener un buen servicio. No solo porque la pyme puede acceder a un especialista que le va a atender con rapidez, sino también porque le va a poder asesorar sobre si pagar el rescate es la mejor solución. La bondad de este producto es que es una herramienta adicional para gerenciar la situación".

No obstante, Macarena Bandrés aclara que "este tipo de gestión siempre forma parte del mismo límite de indemnización, no en adicción".

En el caso concreto de la ciberextorsión o cryptomalware hay que decir que una de cada tres pymes cede a ella. El daño final que causa este tipo de infecciones combina tanto la suspensión de la operativa empresarial como riesgos de reputación y pérdida de datos valiosos. Ahí, Rodriguez afirma que "La extorsión por ransomware es uno de los riesgos con mayor número de siniestros tramitados en la póliza de AIG desde 2013. A estos servicios de resolución tras un incidente, hay que añadir los de prevención para evitar que ocurra el siniestro. Con ellos se detectan vulnerabilidades que se pueden corregir, ayudando a evitar que ocurra. Pero creo que el core de la póliza sigue siendo la responsabilidad civil frente a terceros y los daños propios".

Influencia del Reglamento europeo de Protección de Datos

El nuevo Reglamento europeo de Protección de Datos (que ya está aprobado, pero que entrará en vigor el 25 de mayo de 2018) establece ciertos requerimientos de obligado cumplimiento que se pueden cubrir con una póliza Ciber. Además, como comenta el director de Líneas Financiera para España y Portugal de Chubb, provocará una "evolución de la cultura porque las compañías se plantearán el seguro como una herramienta adicional para trasferir el riesgo y para recibir ayuda. El nivel de diligencia se incrementa y las obligaciones específicas como los gastos de notificación aparecen de una forma clara como algo extra a lo que hay que hacer frente. Es un giro de tuerca adicional e implica una mayor diligencia y proactividad en la seguridad de la información que manejan las empresas con respecto a sí mismas y a sus clientes. Se pasa de una seguridad pasiva a una exigencia proactiva. Las compañías tienen que demostrar que han adoptado todas las medidas. Este cambio de cultura debería de engarzar bien con el hecho de que el riesgo cada vez está más presente y que da igual el tamaño que tengas. Yo soy optimista con el crecimiento del mercado y, sobre todo, con la concienciación que es cada vez mayor". Bandrés considera que "la nueva normativa es beneficiosa para las compañías porque a la larga mitigará el riesgo".

> "El valor añadido de esta póliza, sobre todo para una pyme, es el panel de primera respuesta que da acceso a una serie de servicios que de otra forma no podría tener".
> Luis Moroño

En AIG estamos adaptándonos al nuevo Reglamento europeo tanto para la póliza de Protección de Datos como para la de Ciberriesgo de aplicación a partir del 25 de mayo de 2018. Su CyberEdge Product Leader señala que entre los cambios más significativos de

"El 60% de las pymes no pueden seguir abiertas en los seis meses posteriores a recibir un ataque cibernético. Por eso, es tan importante cubrir bien la pérdida de beneficios, los daños propios y a terceros".
Carlos Rodríguez

la póliza está "que el régimen sancionador se modifica y en lugar de los tres tramos que hay ahora (hasta 600.000 euros), el máximo va a ser un 4% de facturación total o 20 millones de euros. Algo que debe tener en cuenta la aseguradora desde el punto de vista del límite de la póliza. Tendremos que adaptar los límites por sanciones a la exposición real de nuestros asegurados. Además está el proceso de notificación, todas las empresas tienen la obligación de notificar en un periodo de 72 horas a la autoridad de control (describiendo las posibles consecuencias de la violación y las medidas adoptadas) y la notificación a los afectados sin la dilación indebida. Los gastos de notificación pueden llegar a ser costosos si no buscamos vías digitales de comunicar el incidente teniendo la certeza de la recepción y lectura. Otro de los cambios es que ya no va a ser obligatorio inscribir los ficheros en la agencia de protección de datos. Se va a exigir un control interno".

El director en Inerzia Asesores está de acuerdo en que "habrá un gasto de notificación si se produce alguna brecha de seguridad en la base de datos. Algo que para las empresas españolas no era habitual (sí en países anglosajones), porque apenas se aplicaba a empresas de telecomunicación, y ahora se hace real aquí también. A eso hay que añadir el gasto de atender a los clientes que reclamen más información una vez recibida esa notificación. Hay que tener un asesoramiento legal para saber qué tipo de compromiso estás adquiriendo por escrito. También tienes que ser capaz de gestionar la problemática que se les plantea. Generar documentos de preguntas y respuestas frecuentes... hacer esa comunicación eficiente para que no te inunden de una manera que no sea manejable".

En opinión de Javier Ybarra, "está por ver cómo va a evolucionar en estos dos años la forma en que las empresas van a poder cumplir con ese nivel de diligencia extra. Las compañías de servicios especializadas van a trabajar en esa línea. De hecho, hay compañías de certificación que están buscando modelos de certificación para poder ofrecérselos a los clientes; los asesores están muy presentes para ayudar en las revisiones periódicas; las compañías de auditorías... Quizás el mayor impacto va a ser que las compañías tomen más conciencia y dejen la posición pasiva de si me toca veré cómo lo gestiono. Esa situación implica cambios internos en las compañías, medidas proactivas de gestión, buscar personas dentro de tu organización que se hagan responsables... El Reglamento claramente es un incentivo porque un cumplimiento tan fuerte genera oportunidades para todos. Va a haber mayor proactividad".

Respuesta ante el siniestro

Aunque el papel de los corredores es bastante escaso a la hora del siniestro. Carlos Rodríguez indica que "en AIG pensamos que los tramitadores de las correduría tienen que conocer el riesgo y les damos formación para que sepan leer un informe técnico y explicarles cómo actuar ante los incidentes más comunes".

Ybarra afirma que "las aseguradoras especializadas siempre contamos con gente en nuestro equipo interno que coordina el si-

niestro y lo sabe gestionar desde el primer momento. Pero tienes que tener la tranquilidad de que la red de colaboradores externos está bien elegida porque deben dar respuesta desde la línea telefónica que está abierta permanentemente. Como asegurador tenemos que seguir la gestión del proceso en todo momento e intervenir cuando el asegurador tiene que tomar una posición más rápida o más lenta en función de las circunstancias".

La gerente de cuentas de Reaseguros & Wholesale de Howden explica que "nuestra función está más en la concienciación del riesgo y en la contratación de la póliza". En este sentido, el director de Líneas Financiera para España y Portugal de Chubb comenta que "la labor del corredor, como la de otros asesores externos, es hacer entender al cliente el riesgo y saber a qué se enfrenta. Hacéis ese mapa de riesgos para saber qué tiene cubierto y qué no y valoráis junto al cliente si interesa transferir el riesgo".

Rodriguez afirma que "hay que transmitir a la pyme que están autoasegurando el riesgo y si se contrata, va a complementar las pólizas actuales de RC, D&O, Daños, Infidelidad de empleados... También hay que concienciarlas de que no solo está el riesgo del ataque del hacker, que hay más amenazas (un fallo del sistema por un empleado también está cubierto -tanto la negligencia, como el dolo del empleado-; brechas de seguridad de un proveedor tecnológico; el uso ilegítimo de información corporativa; o los gastos de recuperación de los datos por un incendio o inundación, etc.)".

Por todo esto, Javier Ybarra apunta que "el objetivo de comprar una póliza de Ciber es que sea una buena práctica de gestión. No solo implica el pago de indemnizaciones, sino también la capacidad de gestionar esa situación de crisis".

La realidad es que la póliza de Ciber ha ido evolucionando hasta convertirse en una póliza muy completa. Así lo certifica el CyberEdge Product Leader de AIG: "El Ciber es como el hermano mayor de la póliza de Protección de Datos ofreciendo además muchas más garantías y servicios".

"El objetivo de comprar una póliza de Ciber es que sea una buena práctica de gestión. No solo implica el pago de indemnizaciones, sino también la capacidad de gestionar esa situación de crisis".
Javier Ybarra

A esto hay que unir que el precio se ha ajustado bastante en el último año. Luis Moroño señala que, "hoy por hoy, cualquier pyme puede tener una póliza de Ciber por unos 2.000 o 2.500 euros al año. El precio depende mucho de su actividad de negocio y del tipo de datos que maneja".

Además, añade Ybarra, "la forma de contratación se ha simplificado y eso lo hace más fácil a las pymes. Antes se partía de unos cuestionarios muy largos que profundizaba mucho en determinados aspectos que no se conocían. La experiencia que hemos adquiridos los aseguradores especializados nos han permitido simplificarlo mucho para determinados ámbitos de actividad. Son flexibles y se adaptan a cada necesidad".

Carmen Peña
Fotos: Irene Medina

Para leer más sobre la mesa redonda pulse aquí