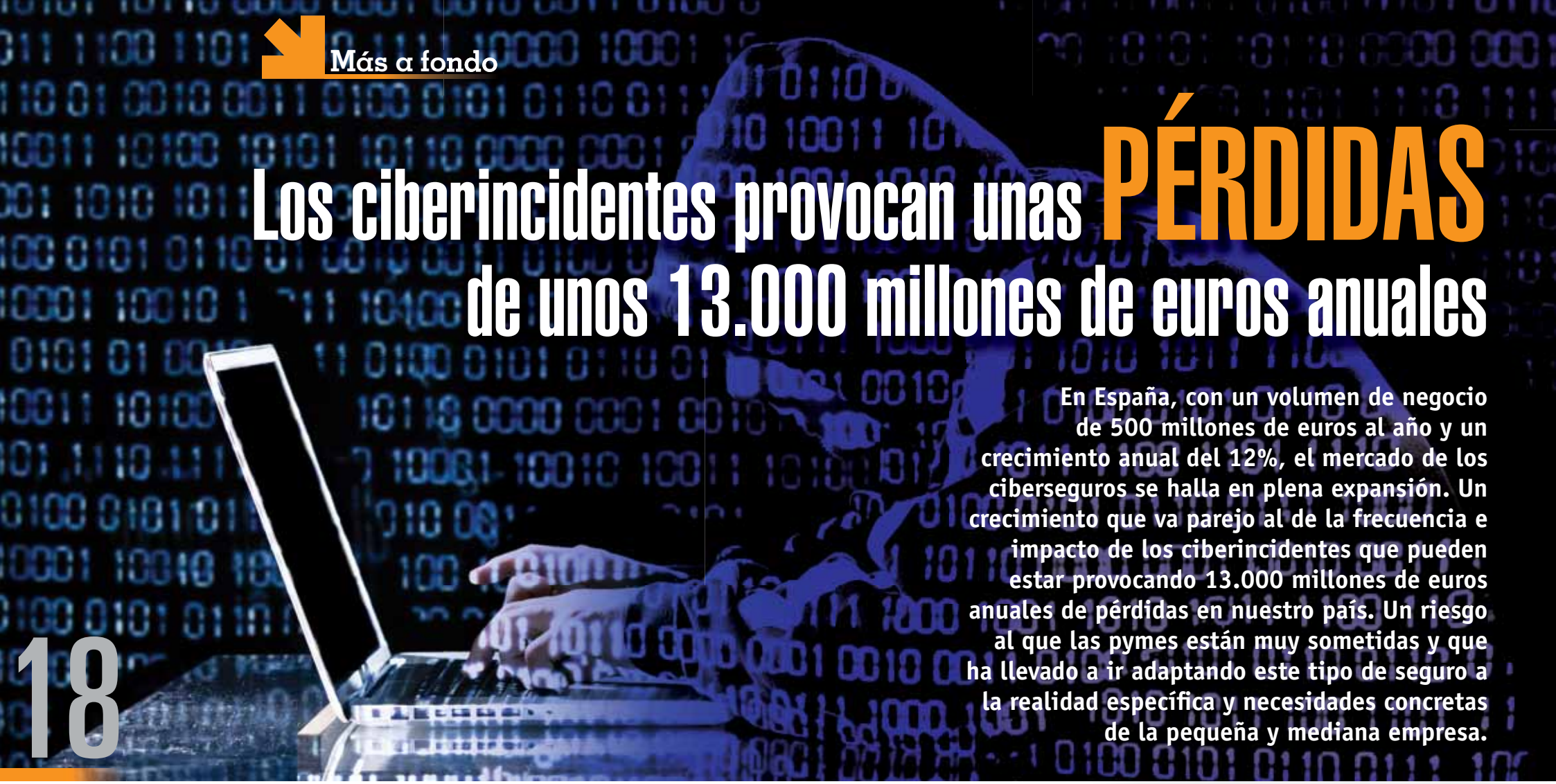
Los ciberincidentes provocan unas PÉRDIDAS de unos 13.000 millones de euros anuales



En España, con un volumen de negocio de 500 millones de euros al año y un crecimiento anual del 12%, el mercado de los ciberseguros se halla en plena expansión. Un crecimiento que va parejo al de la frecuencia e impacto de los ciberincidentes que pueden estar provocando 13.000 millones de euros anuales de pérdidas en nuestro país. Un riesgo al que las pymes están muy sometidas y que ha llevado a ir adaptando este tipo de seguro a la realidad específica y necesidades concretas de la pequeña y mediana empresa.

'Ciberseguros, la transferencia del ciberrriesgo en España' es el nombre del informe que ha realizado Thiber para dar a conocer la necesidad que tienen las empresas (tanto grandes como pymes) de contratar un seguro para hacer frente al riesgo tecnológico que les amenazan. Hoy en día ya no cuestionamos si las ciberamenazas pueden incidir sobre una empresa. La pregunta es cuándo sucederá y si la organización contará con los mecanismos adecuados para hacerles frente.

Prueba de la importancia que está adquiriendo los ciberataques es que se ha impulsado la redacción del nuevo Reglamento Europeo de Protección de Datos y la Directiva Europea 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la inti-

midad en el sector de las comunicaciones electrónicas.

Para intentar contrarrestar los daños que ocasionan los ciberataques, están los ciberseguros. Según el Instituto Nacional de la Ciberseguridad (Incibe), el mercado del ciberseguro en España mueve unos 500 millones de euros anuales, con ritmo de crecimiento anual estimado entorno al 12%. Este crecimiento va parejo al de la frecuencia e impacto de los ciberincidentes. El Instituto de Comercio Exterior (ICEX) apunta que las compañías españolas pueden estar perdiendo más de 13.000 millones de euros anuales como consecuencia de ciberincidentes.

Esas pérdidas se están ocasionando tanto en grandes empresa como en pymes. Por eso, aunque hasta fechas recientes el seguro se había centrado en cubrir las necesidades de las grandes empresas, actualmente este mercado se está orientando al sector de la pyme –con una limitada experiencia en la gestión de estos riesgos, una creciente exposición a los ciberataques y una necesidad de cumplir con un marco regulatorio cada vez más exigente en materia de protección de datos– adaptando su oferta a su realidad específica y necesidades concretas.

Los ciberseguros no sólo permiten transferir el riesgo corporativo a terceros, sino que también promueven la adopción de medidas de ciberprotección más robustas y mejoran la ciberseguridad del mercado, puesto que pueden requerir a sus clientes el cumplimiento de unas cautelas mínimas de ciberseguridad como condición *sine qua non* para la contratación de las pólizas; ofrecer descuentos en las primas a aquellas entidades que demuestren un nivel adecuado de madurez en seguridad; poner en práctica los procedimientos de gestión de ciberincidentes en nombre del asegurado; comprender los patrones de las amenazas y mejorar el intercambio de información entre el gobierno y las empresas aseguradas respecto a ciberincidentes proporcionando una alerta temprana ante este tipo de incidentes.

7.500 millones de dólares en primas en 2020

Es indiscutible que los ciberseguros son uno de los productos de más rápido crecimiento en el mercado asegurador. A medio plazo, éste alcanzará los 7.500 millones de dólares en ventas anuales en 2020 a nivel mundial, frente a los 2.500 millones de dólares del año pasado.

La pyme tiene una limitada experiencia en la gestión de estos riesgos, una creciente exposición a los ciberataques y una necesidad de cumplir con un marco regulatorio cada vez más exigente en materia de protección de datos

En el caso español, este tipo de productos aseguradores comenzaron siendo un traslado de los que se comercializaban en el mercado norteamericano y británico principalmente. Presentaban coberturas y estructuración similar a sus homólogos extranjeros para, paulatínamente, ir adaptándose a la realidad de las empresas españolas. Las compañías internacionales de seguros así como los grandes brokers, debido al profundo conocimiento de estos productos, están liderando esta adaptación a las necesidades nacionales.

El mercado español está compuesto por un gran tejido de pequeñas y medianas empresas (pymes), hecho que las aseguradoras han identificado como una oportunidad de negocio diseñando y adaptando los productos a este sector. El gran reto para llegar a este mercado es el escepticismo del pequeño empresario, que no encuen-

tra necesario adquirir este tipo de seguros, porque considera que los ciberataques son consustanciales a las grandes empresas.

Hay que dejar claro que todas las empresas, con independencia de su tamaño o sector de actividad, tienen algún componente de riesgo cibernético ya que: recopilan, mantienen, ceden o almacenan información privada de carácter personal o confidencial; dependen, en mayor o menor grado, de sistemas informáticos o redes que pueden estar interconectados entre ellos o con otras redes o sistemas de terceros; proveen servicios y productos a través de internet u otros medios electrónicos; contratan con proveedores de servicios tecnológicos (desde mantenimiento, seguridad, gestión de infraestructuras u otros servicios) o con otros proveedores y contratistas independientes para el almacenamiento o tratamiento de la información; pueden estar sujetos a normativa sectorial reguladora de su actividad en cuanto a seguridad de datos o comunicaciones electrónica que implique mayores medidas de seguridad adicionales a las que establece la LOPD; pueden tener obligaciones que cumplir en materia de seguridad frente a la industria de medios de pago; los empleados constituyen el eslabón más débil de la cadena de seguridad de la información; poseen know-how o secretos comerciales en formato digital de los que depende su negocio; y proporcionan algún servicio o producto a terceros que pueden, en caso de ataques maliciosos, constituir los verdaderos objetivos de criminales y atacantes.

El gran reto para llegar a las pymes es que no encuentran necesario adquirir este tipo de seguros, porque considera que los ciberataques son consustanciales a las grandes empresas

Además, las pymes son ahora los objetivos comunes de los ciberdelincuentes, no porque sean lucrativas de forma individual, sino porque la automatización hace que sea fácil de atacar en masa siendo víctimas fáciles (soft targets).

Nuevo escenario de relación con el cliente

En la actualidad, se está produciendo una transición, desde el tradicional ámbito de relación entre aseguradora y asegurado (contratación, pago de la prima, pago de potencial siniestro y renovación o cancelación de la póliza), a un nuevo escenario en que la aseguradora se convierte en proveedor de servicios técnicos y de auditoría continua de los sistemas del asegurado. Esto supone, obviamente, una ampliación de las posibilidades de oferta de tales aseguradoras.

Se pueden hallar seguros enfocados a responsabilidad frente a terceros por vulneración de datos personales o violaciones de seguridad, riesgos regulatorios y gastos diversos, y otros que incorporan coberturas de daños propios (First Party) y que, por lo tanto, dan cobertura a pérdida de beneficios o lucro cesante, robo y otros gastos y pérdidas relacionadas.

No obstante, debe señalarse que el fallo de seguridad no es la única causa de riesgo. Existen otros factores, como puede ser el riesgo de errores humanos, fallos técnicos o de programación, riesgos de difamación o usurpación negligente de propiedad intelectual de terceros o fallo en la cadena de suministro, que pueden ocasionar un perjuicio financiero, interrupción del negocio o un daño reputacional. El informe llama la atención sobre el hecho de que “estas coberturas no suelen ser ofrecidas de forma estándar y hay que negociar normalmente de forma expresa su inclusión en el cuadro del seguro”.

¿Cómo se valora la pérdida de beneficios?

En relación a la pérdida de beneficios existe la problemática asociada a las dos aproximaciones predominantes: el enfoque americano (calcular la pérdida de beneficios hasta que se reinician las operaciones) y el enfoque de pólizas londinense o europeo (hasta el restablecimiento de la producción al nivel normal), así como las dificultades que normalmente encuentran las empresas para separar y cuantificar los factores que inciden en una reducción o aumento de los beneficios esperados que están directamente relacionados con el siniestro.

Pero también hay otras distinciones que son relevantes a la hora de seleccionar un producto frente a otro, como pueden ser la prestación de servicios de consultoría pre-siniestro o los servicios vinculados con la gestión de siniestros.

Los servicios pre-siniestro están muy poco extendidos en España. Ello obedece a varios factores, entre los que se hallan la escasa percepción del valor que pueden aportar estos servicios a las empresas de tamaño medio o grande y, quizá también en vista del escaso interés que suscitan estos servicios, la oferta se limita de forma general a unas horas gratuitas de expertos en materia de seguridad tecnológica y algún dispositivo que combina herramientas

de información de amenazas con herramientas de información.

Estos servicios sin embargo, pueden ser de gran valor en el sector de pequeña y mediana empresa.

De hecho, los pocos productos aseguradores que están viéndose en el mercado español para este sector presentan una aproximación técnica previa para mitigar el riesgo, además de una asistencia técnica especializada cuando ocurre el siniestro.

En el ciberseguro la aseguradora se convierte en proveedor de servicios técnicos y de auditoría continua de los sistemas del asegurado

Exclusiones

Entre las exclusiones que existen de manera general en estos productos, están: los actos deshonestos y fraudulentos y deliberados del asegurado; los daños personales y materiales; las responsabilidades asumidas por contrato o acuerdo; reclamaciones previas y litigios previos e incidentes que hubieran ocurrido (y fueran conocidos) con anterioridad a la fecha de efecto del contrato; infracción de secretos comerciales y patentes; y guerra y terrorismo, a pesar de que a día de hoy existen coberturas afirmativas (o expresas) relacionadas con ataques ciberterroristas. Existe otra exclusión –que puede estar incluida como tal o formar parte de las condiciones generales del contrato y pasar más desapercibida– y es la relativa a datos no declarados o mantenimiento de datos y seguridad por debajo de lo declarado al asegurador durante el proceso de suscripción.

Además, en el informe se plantea que cuando "los riesgos sean considerados como 'no asegurables' por el mercado asegurador privado, se puede considerar la opción de que sea el Estado el que asuma ciertos riesgos para reemplazar o estabilizar el mercado privado, por ejemplo, a través de programas específicos de compensación. En el caso español se podría vehiculizar a través del Consorcio de Compensación de Seguros".