OLIVIER MARCÉN
Responsable de Ciberriesgos de AIG Iberia

"La ciberseguridad afecta a todo tipo de empresas, sea cual sea su tamaño o su actividad"

Licenciado en Derecho por la Universidad Autònoma de Barcelona y acreditado como Certified Information Systems Security Professional, (CISSP), Olivier Marcén lleva más de 15 años trabajando en AIG, donde ha desempeñado distintos cometidos en el departamento de Líneas Financieras. Está especializado en suscripción de Ciberriesgos y Protección de Datos y, en particular, posee un amplio conocimiento del producto CyberEdge.

¿Cuál es la experiencia de AIG en esta materia y en qué consiste su estrategia?
En AIG llevamos más de 20 años suscribiendo Ciberriesgos, primero en Estados Unidos y después en otros países. En muchos casos somos líderes tanto por número de pólizas como por volumen de primas. Nuestro equipo a nivel local, regional y global tiene una amplia experiencia en suscripción y en gestión de siniestros de todo tipo, con independencia de su tamaño y complejidad, que afectan a toda clase de empresas, cualquiera que sea su actividad. Nuestra estrategia de suscripción pasa por asegurarnos de que los clientes cuentan con unas medidas de protección que garanticen su capacidad de resiliencia ante un fallo de seguridad. Dicho de otro modo, queremos tener la certeza de que nuestros clientes cuentan con medidas de seguridad suficientes para detectar y gestionar un incidente de seguridad.

¿Quiénes forman el equipo de Ciberriesgos?
En España el equipo de suscripción está compuesto por cuatro personas: Rafael Ortiz, Yago Armijer, Dani Sánchez y yo, aunque esperamos contar este año con dos nuevas incorporaciones. Recientemente, se ha sumado una persona al equipo de consultoría de Cyber, Vanessa Álvarez, que apoya al equipo global de consultoría de AIG. Además, en Portugal tenemos dos suscriptores multilínea que también se dedican a Ciberriesgos. Claramente, somos el mayor equipo de suscripción del mercado y contamos con un importante conocimiento en esta materia.

¿Se ha incrementado la contratación de pólizas en los últimos años? ¿Cómo afronta AIG el aumento de la siniestralidad?
El ramo de Ciberriesgos es relativamente nuevo y, aunque las empresas suelen contar con pólizas que protegen sus activos físicos, la mayoría de ellas no disponen todavía de un producto específico para proteger sus activos digitales. El volumen de contratación crece cada año, porque está todo por hacer. En cuanto a la siniestralidad, esta se ha disparado en los últimos dos años y algunos informes cifran en 20.000 millones de dólares las pérdidas derivadas de los incidentes de seguridad en 2021. Actualmente, se da la paradoja de que cada vez las empresas quieren contratar más seguros, pero la alta siniestralidad ha provocado un endurecimiento del mercado. Como consecuencia, las empresas que no cuenten con las medidas de seguridad necesarias tienen difícil conseguir contratar una póliza. Sobre todo en algunas actividades, los clientes están demandando límites de capacidad elevados que el mercado asegurador no está dispuesto a ofrecer.

¿El aumento de la siniestralidad puede estar relacionado con la pandemia?
Efectivamente, ahora todo el mundo está mucho más expuesto a los peligros de la red, y más con el teletrabajo, el almacenamiento de datos en la nube,

“La alta siniestralidad ha provocado un endurecimiento del mercado”

etc., porque esos nuevos puestos de trabajo y la arquitectura de red de las empresas no suelen contar con las suficientes medidas de seguridad. Las bandas criminales, cada vez más profesionalizadas, están aprovechando esos agujeros en la red para colarse en los sistemas, encriptarlos, etc.

¿Qué sectores o qué tipo de empresas sufren un mayor número de siniestros?
La ciberseguridad afecta a todo tipo de empresas, independientemente de su tamaño o su actividad. Incluso aquellas compañías que cuentan con unas medidas de protección más sofisticadas pueden padecer también algún tipo de incidente. En realidad, la cuestión no es si voy a sufrir un ciberataque, sino cuándo lo voy a sufrir.

¿Existe suficiente concienciación acerca de la necesidad de asegurar este tipo de riesgos?
Las empresas van tomando conciencia, sobre todo después de padecer algún incidente de *phishing, ransomware,* caídas de sistema, robo de datos… La tipología de siniestros es muy variada. Lo fundamental es que inviertan en mejorar sus controles y políticas de seguridad para garantizar sus activos digitales. Las empresas que sufren un incidente de *ransomware,* por ejemplo, pueden ver totalmente paralizada su producción —al estar sus sistemas conectados a la red— y tener que enfrentarse a reclamaciones de terceros e imposición de multas por parte de la Agencia Española de Protección de Datos. Unas multas que pueden llegar a ser bastante cuantiosas, especialmente en los sectores financiero, de telecomunicaciones y servicios.

¿Cuáles son los siniestros más frecuentes?
Los ataques de *ransomware* se han multiplicado muchísimo, sobre todo en los últimos dos años, y son cada vez más complejos (no tienen nada que ver ya con el WannaCry de 2017). Ahora incluso existe el denominado *ransomware as a service,* es decir, bandas criminales desarrollan un *ransomware* y lo venden como un servicio a otras bandas, que se lucran con este tipo de ataques. También estamos viendo casos de doble o triple extorsión, en los cuales los criminales no se limitan a encriptar los datos de las empresas y pedir un rescate por ellos, sino que, si la víctima no paga, la amenazan con publicar datos confidenciales o, incluso, con facilitárselos a las personas o empresas afectadas.

¿Qué medidas de prevención deberían adoptar las empresas?
Es muy importante que formen a sus empleados para evitar ataques de *phishing.* Además, deben contar con un mecanismo de detección que indique la procedencia de los correos, así como bloquear las visitas a webs que no estén debidamente protegidas. También es

necesario hacer copias de seguridad y almacenarlas periódicamente, además de parchear las vulnerabilidades críticas. Por supuesto, deben contar con antivirus y cortafuegos potentes, sin olvidar la segmentación IT/OT. Asimismo, las cuentas con privilegio de administrador deben ser las mínimas posibles y estar debidamente protegidas, para evitar que los criminales puedan acceder al sistema y navegar libremente por él.

¿En qué consiste CyberEdge?
Nuestro producto se basa en tres pilares fundamentales: la prevención, la capacidad de respuesta y la propia póliza como tal. Por lo que respecta al primer pilar, ponemos a disposición de nuestros clientes —e incluso de quienes no son clientes nuestros— una serie de servicios de prevención. A partir de un cuestionario inteligente, nosotros les proporcionamos un informe de madurez antes incluso de contratar la póliza. En él, cuantificamos las pérdidas que pueden ocasionar distintos tipos de incidentes, medimos el riesgo implícito y explícito, etc. Una vez contratada la póliza, ese informe se amplía mucho más y añadimos otros servicios, como cursos *online* de formación y concienciación para los empleados, análisis de vulnerabilidades del sistema o la posibilidad de contratar servicios de consultoría.
En el segundo pilar se incluye la consultoría de primera respuesta, que se activa cuando un cliente sufre un incidente de ciberseguridad y necesita asesoramiento durante las primeras 72 horas. El objetivo es comprobar si el fallo de seguridad sigue existiendo y cómo se puede detener, así como determinar sus implicaciones legales.
Respecto al tercer y último pilar, cabe destacar que las coberturas y definiciones de nuestro producto —por ejemplo, en cuanto a oferta externa de servicios, fallos de interrupción de red o fallo de sistemas— son de las más amplias del mercado, incluyendo coberturas por pérdida de beneficio, responsabilidad de terceros, ciberextorsión, etc.

¿Y qué ocurre con este tipo de riesgos en las pólizas de otros ramos?
Nosotros somos muy claros y queremos que el cliente entienda siempre qué coberturas tiene contratadas. Por eso, creemos que es muy importante que en las pólizas de Daños, Responsabilidad Civil, Transportes e, incluso, Responsabilidad Civil Profesional, haya una cobertura afirmativa o una exclusión específica de Ciberriesgos.

¿Cuál es el papel de los *brokers* en materia de ciberseguridad? ¿Reciben formación por parte de AIG?
El papel de los *brokers,* como no podía ser de otra manera, es fundamental. Y más en un contexto como el actual, de incremento de la siniestralidad y dificultad para acceder a un seguro de Ciberriesgos. Los *brokers* deben explicar a las empresas que, para poder transferir sus riesgos a una aseguradora, tienen que contar con unas mínimas medidas de seguridad.
En ese sentido, la formación de los corredores es primordial para nosotros. Por ello, todos los años celebramos determinados eventos —ahora en formato *online*— no solo para explicar las coberturas de la póliza, sino también para concienciar acerca de las ciberamenazas y analizar en casos reales cómo responde este seguro.