NUEVO PRODUCTO: CIBERRIESGOS

EL FUTURO ES HOY

Si miramos hacia atrás, muchos de los actos que hoy forman parte de lo cotidiano, o de nuestra rutina diaria, antaño probablemente pensaríamos que hablábamos de pura ciencia ficción. Pedirle al coche llamar a casa, desbloquear el móvil utilizando la huella digital o guardar todos los archivos en una nube digital, son algunos de los cientos de ejemplos que hoy nos parecen normales y que hace «no mucho tiempo» habríamos pensado que formaban parte del guión de *Men in Black*.

Las nuevas tecnologías avanzan a una velocidad de vértigo, y el mundo con ellas. Afectan a todos; personas, gobiernos, pequeños comercios y grandes corporaciones y han cambiado por completo la forma en que nos relacionamos. Desde las aplicaciones de mensajería instantánea a la presentación telemática de documentos oficiales, pasando por todas las plataformas o redes sociales. ¿Alguien se acuerda de las avionetas sobrevolando las playas con los anuncios colgando?

Todos los avances tecnológicos tienen, por norma general, un principio o denominador común, son creados para hacer más fáciles, más rápidas y (a menudo) mejores, muchas de las tareas del hombre, de los animales y de la naturaleza.

Esta afirmación, a priori positiva, conlleva también a otra reflexión fuera de las discusiones éticas: Nuevos escenarios, nuevos riesgos.

El escenario patrimonial de las empresas ha cambiado de forma significativa. Los bienes intangibles cada vez tienen un mayor peso y relevancia frente a los bienes tangibles. Este cambio requería un replanteamiento acerca del

papel del seguro tradicional, que estaba centrado en dar soluciones, principalmente, en la transferencia de riesgos sobre los bienes tangibles dejando un vacío significativo en cuanto a los intangibles.

La velocidad con que se generan los cambios en los escenarios, ha provocado que la percepción de los nuevos riesgos, los que podríamos llamar los «ciberriesgos», se haya quedado alejada del alcance real de estos.

Actualmente podemos decir que, en el ámbito de las grandes multinacionales, esta distancia empieza a acortarse. En la última encuesta realizada en el *World Economic Forum* acerca de los principales riesgos que afectan a la economía, los ciberataques ya se sitúan entre los cinco de mayor preocupación.

En artículos recientemente publicados en los medios especializados, se percibe un discurso más maduro por parte de los principales Risk Managers Europeos. En este sentido, se pone de manifiesto la necesidad de una concienciación amplia por parte de la empresa en la que se implique activamente la alta dirección. Por otro lado, se demanda a la industria del seguro soluciones a medida que se adapten a la complejidad de los nuevos riesgos.Ya no podemos, ni debemos, hablar de un riesgo emergente ni de un problema acotado solamente a las áreas de IT de las empresas. Nos encontramos en una fase en la que, tanto los Brokers, como las compañías de seguros y los Risk Managers empiezan a coordinarse y están obligados a entenderse.

El creciente número de ciberataques (España es el tercer país del mundo por detrás de EE. UU. y Reino Unido) en los que se generan unas pérdidas anuales para las compañías por encima de los 14 mil millones de euros, el considerable aumento de coste medio por incidente, que pasó de 0,5 millones de euros en 2012 a 0,8 millones de euros en 2013, con un coste medio anual por empresa de casi 9 millones de euros, están poniendo a las inversiones en tecnología como uno de los puntos prioritarios en las agendas de las compañías, aunque todavía queda un largo recorrido en lo que atañe a la pequeña y mediana empresa.

En este sentido, según el *Cost of Cyber Crime Study,* publicado por el Instituto Ponemon en el 2014, se pone de manifiesto el alto retorno sobre la inversión en las principales tecnologías de seguridad, tales como sistemas de encriptación (18%), sistemas de inteligencia en seguridad (21%) o perímetros de control avanzados firewall (15%).

La mayoría de los siniestros de gran intensidad provienen del mercado americano (Target, Anthem, Home Depot) y principalmente derivan de violaciones de seguridad que afectan a grandes bases de datos personales.

Cabe reseñar que el mercado estadounidense ha sido pionero en cuanto a las coberturas de ciberriesgos como respuesta a las particularidades de la normativa local que regula las indemnizaciones relacionadas con la protección de estos datos.

En el caso concreto de Target, una de las mayores cadenas de supermercados de Estados Unidos, en el que los ciberdelincuentes robaron datos financieros y personales de 110 millones de clientes colándose en los sistemas de la compañía a través de un pequeño proveedor de servicios de refrigeración, se puso de manifiesto la necesidad de contar, no solo con unas medidas de seguridad propias, sino también con la necesidad de controlar que los proveedores externos, que tengan acceso a información sensible, tomen las mismas medidas.

No obstante lo anterior, y fuera de las peculiaridades del mercado en Estados Unidos, dentro de las consecuencias derivadas de las ciberamenazas, cada vez cobra más importancia el impacto generado por la interrupción de negocio en las empresas.

La operativa de la gran mayoría de las empresas depende, principalmente, de sus sistemas informáticos. Un ataque o fallo de estos puede provocar un auténtico caos interno con las posibles implicaciones de contagio en los mercados. De esta suerte, todas las medidas de seguridad, no solo deben ir dirigidas a la protección de información sensible, sino también a proteger y garantizar la continuidad del negocio.

La variedad de actores que forman el cuadro de las ciberamenazas (ciberespías, ciberdelincuentes, hacktivistas, terroristas o, incluso, personal propio de las compañías) y la creciente sofisticación de las herramientas y métodos de ataque que utilizan (*phishing, malware, exploits*…), hacen que nadie esté fuera de peligro. Apenas hace unos días se acaba de publicar que unos hackers han «asaltado» las bases de datos de la Agencia de Personal del Gobierno de Estados Unidos, y han sustraído una importante cantidad de datos personales de empleados federales.

Ante este panorama, y a pesar de encontrarnos en una etapa en la que se está avanzando desde un punto de vista legislativo para adaptarse a estos nuevos escenarios, la palabra clave que hay que subrayar es la «prevención».

Como se ha comentado anteriormente, el desarrollo del papel de la industria del seguro en la prevención de estos nuevos riesgos representa una oportunidad de negocio en la que tendrán una ventaja competitiva aquellas compañías que sepan escuchar y adaptarse mejor a las necesidades del cliente.