El seguro de Ciber es cada vez más una necesidad

Verónica Jiménez // Head Cyber Insurance España (AON)
Pablo Montoliu // Chief Information & Innovation Officer (AON)
José J. Martínez // Universidad de Alcalá

Es indiscutible que la ciberseguridad se ha convertido en los últimos años en una de las mayores preocupaciones de las empresas, debido al incremento tan significativo de ciberataques sufridos durante las últimas dos décadas.

El 2020 y la pandemia han afectado drásticamente la ciberseguridad y han impulsado un cambio significativo dentro de las organizaciones. Las restricciones gubernamentales han significado que una gran cantidad de empleados tengan que trabajar de forma remota a largo plazo y las empresas de todos los sectores han tenido que adaptarse para sobrevivir.

Los ciberdelincuentes han aprovechado esta circunstancia para incrementar tanto el número como la sofisticación de los ataques. Casi podemos hablar de otra pandemia que ha irrumpido con más fuerza en estos momentos: ataque *ransomware* y el fraude por ingeniería social.

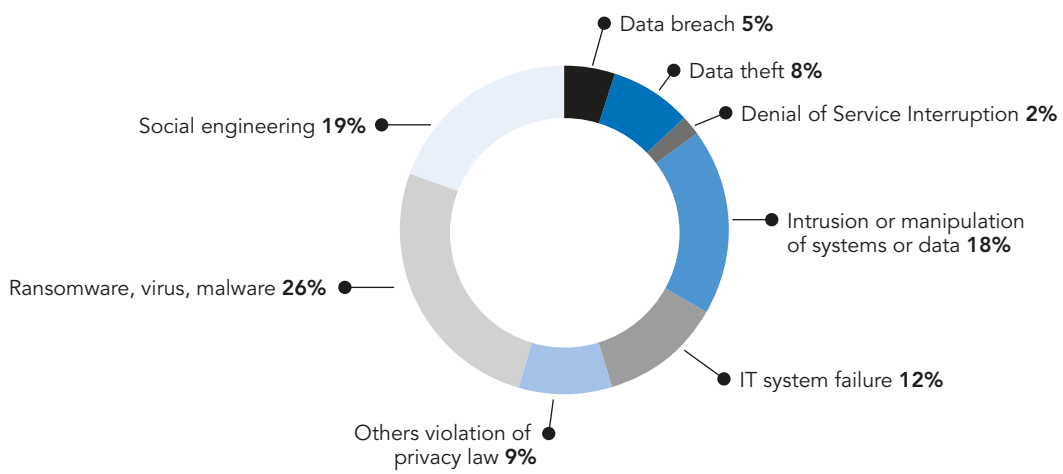
Internet es un entorno donde el fraude y el crimen organizado actúan más de lo que a menudo se percibe, aunque con herramientas diferentes a las tradicionales. Por ejemplo, es posible desarrollar estafas en cualquier red social utilizando ingeniería social y manipulación.

Los ataques con programas maliciosos, los de denegación de servicios o los efectuados con *ransomware* son recursos que utiliza comúnmente el crimen organizado. Uno de los objetivos habituales de estos delincuentes son los datos, que tratan de robar o secuestrar a cambio de grandes sumas de dinero. Y, para lograr sus objetivos, se valen de las vulnerabilidades en los sistemas informáticos de las empresas.

No obstante, también hay que tener en cuenta la ingeniería social mencionada. Los propios empleados de una compañía pueden convertirse en un punto débil si carecen de la formación adecuada.

Adicionalmente, trabajar de forma remota crea una gran variedad de problemas de seguridad, por ejemplo, acceder a archivos de trabajo y completar tareas en dispositivos personales o redes domesticas es muy peligroso. Por otra parte, es más probable que el personal que trabaja de forma remota utilice los dispositivos corporativos para realizar actividades personales, como compra *online*, navegación por internet o

Figura 1: Causa de siniestros



Fuente: *Data Analytics Aon.*

transacciones financieras, lo que también significa un riesgo para las empresas, ya que amplían el área de amenaza para que los cibercriminales la exploten.

Aunque no son las únicas formas de ataque, sí que podemos afirmar que son las que más impactan en la siniestralidad de las pólizas, tal y como se ve en el gráfico a continuación, donde el ataque malicioso, el fraude por ingeniería social y el robo o la manipulación de datos, constituyen casi el 80% de los siniestros sufridos y los que generan mayor impacto económico.

En España empezamos a vivir en nuestras propias carnes ataques *ransomware* muy conocidos como Wannacry, not petya o ryuk, si bien no fue hasta finales de 2020 y principios del 2021 cuando hemos empezado a observar ataques con impactos económicos muy significativos en empresas españolas.

> Desde 2012, año que se firma en España la primera póliza Cyber, hasta ahora, los condicionados han ido cambiando conforme las coberturas han ido evolucionando para adaptarse a nuevos escenarios bajo el riesgo cibernético

Todos estos ataques han tenido también un impacto sobre el mercado asegurador, por dos motivos principales, el primero y más directo, es que muchas de las empresas que han sufrido estos ataques tenían contratadas pólizas de ciberriesgo que han asumido la mayor parte de las pérdidas ocasionadas, y el segundo motivo, es que las previsiones de los expertos de ciberseguridad indican que el 2021 vamos a continuar con "más de lo mismo" o si esperamos algún cambio será hacía una sofisticación y gravedad de los ataques. Por un lado, el *ransomware* con exfiltración de información seguirá marcando el paso en el día a día de los ciberataques, y en algunos casos, combinado con la doble extorsión de la publicación de la información exfiltrada.

Desde 2012, año que se firma en España la primera póliza Cyber, hasta ahora, los condicionados han ido cambiando conforme las coberturas han ido evolucionando para adaptarse a nuevos escenarios bajo el riesgo cibernético.

El objeto principal de los ciberseguros es mitigar el impacto económico de pérdidas y gastos varios que se generan al sufrir un incidente crítico –impacto que puede ser pérdida y gastos propios, de terceros o por causa regulatoria–, a la vez que ayudan a la empresa a gestionar estos incidentes mitigando asimismo la pérdida reputacional con los servicios que el asegurador pone a disposición del asegurado para la respuesta/gestión de incidentes. Las coberturas del seguro se dividen en tres bloques principales:

- **Servicios de asistencia o respuesta ante incidentes:** Se cubre los costes y gastos para gestionar el incidente y sus consecuencias. Fundamentalmente, gastos forenses de investigación, gastos de reconstrucción de datos, gastos de respuesta a afectados por un compromiso de datos personales (notificación, establecimiento de *call centers*, servicios de monitorización de crédito, seguros de robo de identidad, etc.) y gastos de publicidad/gestión de crisis mediática en caso de que el incidente aparezca en los medios de comunicación y con la finalidad de minimizar el daño a la imagen del asegurado.
- **Daños propios:** pérdida de ingresos o extracostes derivados de daño inmaterial o gastos en caso de extorsión cibernética.
- **Responsabilidad civil frente a terceros:** daños, perjuicios y gastos de defensa frente a reclamaciones de afectados por una violación de datos o por los perjuicios sufridos a consecuencia de una quiebra en la seguridad de los sistemas.
- **Procedimientos regulatorios:** En caso de un compromiso de datos personales, si el regulador abre una investigación formal, la póliza cubre los costes y gastos de asesoramiento legal de las personas que deban comparecer, así como también, la posible sanción administrativa.

Durante los primeros años, y hasta el año 2020, hemos visto que las compañías estaban dispuestas a mejorar el alcance de las pólizas, ampliando coberturas: Ampliación de la Pérdida de beneficios a fallos de sistema, por pérdida de confianza de los clientes tras un ciber ataque; Transferencias fraudulentas, Cupones descuento, etc.

Este tipo de pólizas sigue evolucionando, pues tengamos en cuenta que un siniestro cyber también puede afectar a pólizas tradicionales como D&O, Responsabilidad Civil Profesional, Todo Riesgo Daños Materiales, Transportes, etc. Cada vez toma más peso el "Silent Cyber" y se están incluyendo exclusiones espe-

cíficas de eventos cibernéticos en el resto de los ramos de seguros, es decir, el mercado asegurador cada vez tiene más definido que las consecuencias económicas de un evento cyber se quieren cubrir a través de una póliza específica.

Lamentablemente los tiempos de gloria donde existía exceso de capacidad, mucha competencia y precios competitivos en el mercado español para la contratación del seguro han pasado, y desde enero de 2021 estamos observando las consecuencias de todos los cambios que hemos estado comentando, así como la siniestralidad que se está produciendo. Las aseguradoras han tenido que tomar medidas drásticas para rentabilizar el ramo y que continúe siendo una línea viable en el tiempo.

Estas medidas son comunes a todas las aseguradoras y dentro de ellas destacamos:

- Incremento significativo en tasas y franquicias.
- Suscripción muy rigurosa, cada vez se exige más información a los asegurados.
- Reducción de la capacidad: hay aseguradores que se han retirado y los que siguen suscribiendo han reducido la capacidad disponible.
- Modificaciones en las cláusulas, que afectan principalmente a dos de las coberturas que se han visto gravemente impactadas por los siniestros: extorsión cibernética y pérdida de beneficios derivada de un fallo de seguridad.
- Se incluyen nuevas exclusiones como consecuencia de la siniestralidad tramitada.

Las empresas gestionan el riesgo cibernético desde 3 perspectivas sin dejar de lado ninguna de ellas:

- Desde la Ciberseguridad, como enfoque preventivo. Ninguna empresa tiene un sistema informático infalible y todas establecen ya sus presupuestos económicos para invertir en protección de sistemas y los equipos de Seguridad.
- Desde el cumplimiento normativo, en cuanto a que la legislación cada vez es más severa: el Nuevo Reglamento en materia de protección de datos establece nuevas obligaciones frente a un compromiso de datos y eleva el importe de la sanción más grave; así como la Ley de Sociedades de Capital establece que el riesgo tecnológico es un riesgo de negocio y como tal es competencia de la alta dirección tomar parte activa en su gestión.
- Desde el programa de seguros ciber entendido este como una herramienta de mitigación: si al final sucede el ciberincidente, es necesario contar con una póliza que compense las pérdidas y contribuya a la sostenibilidad del negocio.

Por tanto, el seguro debe verse como parte de un enfoque integrado de ciberseguridad. Invertir en seguro no reducirá el riesgo de sufrir un ciberataque, sin embargo, es importante recordar que la mayoría de las herramientas de ciberseguridad son medidas preventivas y las empresas deben revisar también que medidas de respuesta a incidentes tienen implementadas y que dichas medidas funcionen en el desafortunado caso de sufrir una brecha de seguridad. Es en este punto, donde el seguro cada vez toma mas peso y se convierte en una de las soluciones de mitigación y respuesta frente a un ciberataque, siendo una pieza fundamental que ayuda a cerrar el círculo de la gestión del riesgo cibernético.

Hace unos años la frase más escuchada y repetida era "hay dos tipos de empresas, las que han sufrido un ataque y las que lo van a sufrir", hoy en día, esta afirmación no se pone en duda, ni tampoco que el seguro de Ciber ha dejado de ser un "capricho" para ser una necesidad para las empresas. ●

Foto: iStock.com/Sergey Shulgin