# LOS RIESGOS CIBERNÉTICOS

Hoy en día es mucho peor perder el teléfono celular que la billetera. Sin el celular a mano no es posible efectuar operaciones tan disímiles como transacciones bancarias, compras electrónicas, participar en reuniones virtuales, ingresar a la propia oficina o, simplemente, mantenerse al día de los acontecimientos de la jornada. Si a lo anterior se añade el riesgo de perder toda la información almacenada en esos dispositivos, las consecuencias derivadas de su pérdida o hurto son graves. De hecho, hay compañías de seguros que se especializan en asegurar celulares contra daños físicos y robos. Según Interpol, el robo de teléfonos móviles es uno de los delitos más comunes en Latinoamérica y mueve en promedio US$550.000 diarios en la región. Sólo como un dato ilustrativo, en la Región Metropolitana se denuncian más de 200.000 robos de teléfonos celulares al año.

Lo anterior es fiel reflejo de la relevancia que ha adquirido la tecnología en la vida diaria y los riesgos asociados a este fenómeno. De hecho, informes especializados califican la protección de datos y ciberseguridad como el riesgo más relevante que debe enfrentar el mercado reasegurador. Es cuestión de recordar el evento que enfrentó el Banco de Chile, que causó la paralización de sus operaciones por algunos días debido a un hackeo a las cuentas corrientes. Sin ir más lejos, a comienzos de mes, la Unión Europea acusó a Rusia de un ciber ataque contra el satélite KA-SAT Network el cual alteró las comunicaciones en Ucrania y otros países miembros de la Unión Europea, y cortó el acceso a 5.800 aerogeneradores en Alemania. De hecho, se estima que el costo a nivel mundial causado por cibercrímenes llegó a seis billones de dólares el año 2021.

Por lo mismo, los seguros que cubren riesgos derivados de la ciberseguridad o de la operación de softwares han experimentado una evolución aceleradísima. Las pólizas existentes en el mercado cubren los riesgos de virus y malware, filtración de datos sensibles y la interrupción de servicios tecnológicos. Normalmente quedan sin cobertura los riesgos cibernéticos que afectan a la operación de infraestructura crítica, tales como generadoras nucleares, embalses, plataformas de transacciones financieras, canales, etc.

En un principio, sólo se aseguraban los daños físicos que pudieran afectar a terminales, redes y servidores. Pero en la medida que el uso de la tecnología se expandió y el valor de la información almacenada en medios digitales creció, la necesidad de cubrir riesgos asociados a esas actividades se ha amplificado a niveles insospechados.

En general la cobertura de riesgos cibernéticos empieza por proteger la infraestructura lógica y física. Sobre esa cobertura se construye el resto de la estructura de seguros que protege contra los diversos riesgos que forman parte de este ramo, tales como robo de información, ransomware, filtración de datos, perjuicios por paralización, daños a la imagen de los asegurados a consecuencia de la ocurrencia de esos riesgos, responsabilidad civil por mal uso de los datos, cyber extorsión, etc. El listado de riesgos es grande y va evolucionando en la medida que cambian los modelos de negocio y aparecen nuevos tipos de fraudes informáticos.

En el proceso de evaluación de los riesgos cibernéticos de una compañía normalmente se llega a la conclusión que es necesario actualizar equipos, servidores, softwares, firewalls, etc. Es probable que dicha inversión sea costosa pero rentable, porque disminuye la ocurrencia de incidentes o su intensidad, a la par que elimina en buena medida el riesgo de una paralización de actividades y la larga cadena de consecuencias financieras.

Por último, es recomendable que en la evaluación de riesgos y la negociación de las coberturas de seguros relacionados con ransomware, protección de datos, perjuicios por paralización, etc., las compañías se asesoren adecuadamente. En los seguros tradicionales la identificación de los riesgos y sus consecuencias económicas son más evidentes. Sin embargo, en riesgos de esta naturaleza las consecuencias son mucho más amplias, en cuanto al territorio, número de personas afectadas o perjuicios económicos sufridos. Por ejemplo, una multinacional chilena con operaciones en la Unión Europea, que sufra una filtración de datos personales sensibles que afecten a ciudadanos de países miembros de la Unión Europea puede verse expuesta a multas muy relevantes. O una compañía chilena que tomó una cobertura circunscrita al territorio de Chile puede quedar sin cobertura si el incidente que la afectó se produjo en un servidor ubicado físicamente en el extranjero.

## CONTACTO

Patricio Prieto L.
Socio
pdprieto@prieto.cl