¿Están los directivos preparados frente a los ciberataques?

by María García Muñoz, abogada senior en Muñoz Arribas Abogados, S.L.P

Por
Colaborador
-
26 octubre, 2022

Hace pocos días, Lloyd's sufría una incidencia cibernética que le llevó a tomar la difícil, pero acertada, decisión de desconectar todos sus sistemas informáticos. Lloyd's cortó toda la conectividad externa, incluidas las plataformas de autoridad delegada. Esto supuso el bloqueo de los sistemas de Lloyd's, lo que ha afectado también a los sindicatos y compañías aseguradoras del mercado londinense.

Cuando sufrimos un **ciberataque**, lo más probable es que este también afecte a su **cadena de proveedores.** Una organización afectada por un incidente cibernético puede sufrir daños propios, pero con casi total seguridad podría provocar daños a terceros.

Desde el punto de vista del seguro, debemos tener en cuenta que la responsabilidad de los Administradores y Directivos puede, o no, estar cubierta en la póliza de D&O así como por el seguro de riesgos cibernéticos.

Desde la Alta Dirección se debe dar prioridad a esta cuestión, ya que el impacto que puede sufrir una compañía por un incidente cibernético en sus sistemas informáticos puede tener **graves consecuencias tanto financieras como pérdidas económicas directas entre otras,** daño reputacional, responsabilidad civil frente a terceros perjudicados, incluso, como estamos viendo en la actualidad, la imposición de elevadas sanciones.

Si a ello añadimos un **entorno regulatorio** cada vez más complejo y con multas más elevadas, no es de extrañar la preocupación creciente que genera esta materia en los Consejos de Administración.

La responsabilidad de ello recae en el **Administrador y/o Altos Directivos, que también responden conforme al artículo 1.903 del Código Civil** de sus propios dependientes, sin perjuicio de la facultad de repetición de aquellos.

Hay que tener en cuenta que **los órganos de administración serán los responsables últimos.** Por ello, deben de emplear cuantos medios sean necesarios para garantizar la integridad cibernética, entre otros:

- Conocer e identificar el riesgo y elaborar la Evaluación de Riesgos.
- Incorporar la ciberseguridad en el Plan Director de Seguridad.
- Formar y concienciar a la plantilla de empleados.
- Revisar y actualizar nuestros procedimientos y medidas para mitigar la exposición al ataque.
- Incluir en la política de la compañía, la inversión y renovación de los sistemas de IT de la compañía.
- Gestionar los incidentes a través del desarrollo y control de políticas de actuación frente a un ciberataque: Plan de Respuestas ante incidentes y Plan de Contingencia y Continuidad de Negocio.

Desde el punto de vista del seguro, debemos tener en cuenta que la responsabilidad de los Administradores y Directivos puede, o no, estar cubierta en la **póliza de D&O** así como por el seguro de **riesgos cibernéticos.**

Los brókers son actores importantes para asesorar sobre la priorización y cuantificación en los ciberriesgos de las empresas, tan importante es conocer los riesgos a los que una compañía están expuestos como saber cuál es la estrategia adecuada.

Por ello, a la hora de contratar un seguro que pueda conseguir mitigar el impacto de los ciberataques, **debemos tener en cuenta que cubra**, entre otras, la interrupción de servicios, la destrucción de datos, los riesgos derivados de la privacidad de dichos datos, así como el daño reputación que estas brechas ocasionan a las compañías y la responsabilidad de los Altos Directivos. El seguro contra riesgos cibernéticos o de responsabilidad cibernética nos da, no solo una respuesta, sino la garantía para mantener el negocio en funcionamiento y salvaguardados frente a los posibles daños ocasionados a los terceros vinculados a nuestro negocio.

En conclusión, es fundamental para los Administradores y Directivos contar con pólizas, tanto de riesgos cibernéticos como de D&O y que ambas estén coordinadas de cara a cubrir las responsabilidades de estos.

Sobre el autor del artículo