beazley

La responsabilidad recae en la Junta Directiva: Responsabilidad ante el ciberriesgo

Rory Burling

La mala gestión de un incidente cibernético es un riesgo creciente en todo el sector de los seguros de responsabilidad civil. Desde una filtración de datos hasta ciberataques mal gestionados, los ejecutivos se enfrentan a una creciente exposición a litigios relacionados con incidentes relacionados con la ciberseguridad.

Las vulnerabilidades cibernéticas deben ser gestionadas de forma adecuada.

Las vulnerabilidades cibernéticas deben verse a través de una lente de riesgo ejecutivo. Si una empresa es víctima de un ciberataque, el impacto podría ser de gran alcance, desde la caída del precio de las acciones hasta las pérdidas por interrupción de la actividad y el daño a la reputación.

La ciberseguridad es una de las principales amenazas para las empresas.

A medida que la innovación tecnológica continúa a buen ritmo, los ciberdelincuentes se están volviendo más sofisticados y audaces en su enfoque. En el segundo trimestre de 2024, Check Point Research observó un **30%** de aumento interanual en los ciberataques a nivel mundial . A la luz de esta tendencia, es inevitable un aumento de los litigios centrados en el riesgo cibernético. Para contrarrestar esta amenaza, las empresas necesitan:

- Planes de continuidad de negocio ensayados con regularidad que incluyan la gestión de crisis y de la reputación
- Un buen conocimiento de los proveedores externos y de la dependencia y conectividad de las empresas con ellos

- Un programa de seguro cibernético adecuado con experiencia en la gestión de reclamaciones

.

Todos los elementos anteriores deben gestionarse activamente con las principales partes interesadas de toda la empresa, de modo que si ocurriera lo peor, los clientes y sus aseguradoras puedan gestionar la situación y mitigar el riesgo de forma rápida y adecuada. Unos procedimientos sólidos de gobernanza interna y de marco de riesgos para comprobar la existencia de infracciones y la notificación lo antes posible a las aseguradoras una vez que se ha producido una infracción también son primordiales para mitigar un incidente de infracción cibernética.

Ranking cyber risk in a chaotic global landscape

Cuando los ejecutivos se enfrentan a un creciente escrutinio sobre cómo gestionan el riesgo cibernético, nuestro estudio Risk & Resilience realizado con ejecutivos de todo el mundo reveló que **el 23%** no se siente preparado para hacer frente a las amenazas que plantea el riesgo cibernético. Sin embargo, resulta alentador que el **24%** esté pensando en invertir en defensas de ciberseguridad para ayudar a aumentar la resistencia ante este riesgo.

Entre los muchos retos a los que se enfrentan nuestros ejecutivos globales encuestados, **26%** clasificó el riesgo cibernético como su principal riesgo de preocupación este año. Se trata de una cifra considerable que es probable que aumente dado el incremento del número de ataques y el creciente escrutinio que están aplicando los reguladores en este espacio.

Un enfoque de espectro completo

Un enfoque de espectro completo de la ciberseguridad implementa medidas preventivas y preventivas, como la exploración del horizonte de riesgo para identificar los puntos ciegos de riesgo y las amenazas emergentes. Al hacerlo, forma parte de una estrategia más amplia de mitigación de riesgos que puede ayudar a tranquilizar a los inversores y promover las mejores prácticas internamente.
Si un ataque cibernético lleva a los inversores a cuestionar la competencia de la junta directiva, los ejecutivos pueden defenderse con pruebas tangibles de que se tomaron medidas razonables para evitar que el ataque ocurriera en primer lugar, y demostrar que tenían planes activos de gestión de riesgos y apoyo para ayudar a mitigar el impacto del ataque.

En la actualidad, la ciberseguridad es una de las principales amenazas para la empresa.

En el impredecible panorama de riesgos actual, las aseguradoras pueden desempeñar un papel fundamental compartiendo información sobre reclamaciones y normativas, y proporcionando coberturas completas y personalizadas que ayuden a responder y mitigar los riesgos cibernéticos y de D&O a los que se enfrentan.

En última instancia, el riesgo en una empresa recae en el consejo de administración, y no garantizar la seguridad de sus sistemas podría

causar problemas a largo plazo. En caso de que una empresa sea víctima de un ataque que comprometa datos confidenciales y provoque una reducción del precio de las acciones, pérdida de ingresos y daños a la reputación, tanto la empresa como sus directivos tendrán que dar la cara ante sus accionistas, inversores y clientes.

El riesgo en una empresa recae, en última instancia, en el consejo de administración, y no garantizar la seguridad de sus sistemas podría causar problemas a largo plazo.

Rory Burling

Underwriter - Specialty Lines – International Management Liability

beazley