Los nuevos requisitos de la SEC (Securities and Exchange Commission) deberían impulsar la revisión de los marcos de ciberseguridad y la cobertura de seguros D&O

Lockton México | 2023

LOCKTON®

El mes pasado, la **Securities and Exchange Commission (SEC) anunció nuevos requerimientos para que las empresas públicas en EE.UU. revelen los riesgos materiales de ciberseguridad** más rápidamente y con mayor detalle, además de divulgar proactivamente detalles sobre sus prácticas de gestión de riesgos de ciberseguridad. La norma deja claro que la SEC espera que las empresas públicas den prioridad a la ciberseguridad y, como cualquier nuevo requisito, crea riesgos que las organizaciones deben considerar cuidadosamente y estar preparadas para gestionar.

Notificación de incidentes materiales de ciberseguridad

El 26 de julio, la SEC **finalizó su norma sobre gestión de riesgos de ciberseguridad de las empresas públicas,** gobernanza y notificación de incidentes. En virtud de la nueva norma, **propuesta inicialmente en marzo de 2022,** las empresas que cotizan en las bolsas de EE.UU. están obligadas a revelar a los inversionistas cualquier incidente material de ciberseguridad, incluyendo el suministro de información sobre la naturaleza, el alcance, el momento y el impacto material o la probabilidad de impacto material de esos incidentes.

La compañía está obligada a hacer tal divulgación dentro de los cuatro días siguientes a una determinación de materialidad, a menos que el fiscal general de EE.UU. haya determinado - por escrito - que la divulgación supondría un riesgo sustancial para la seguridad nacional o la seguridad pública. La determinación de la materialidad debe hacerse "sin demora injustificada".

La norma también exige a las compañías que:

- **Describan dentro de los reportes trimestrales y anuales** sus prácticas de gestión de riesgos cibernéticos, incluidas las políticas para evaluar, identificar y gestionar los riesgos materiales. En su caso, las empresas también están obligados a revelar cómo se integran estas políticas en las funciones generales de gestión de riesgos de sus organizaciones, cualquier tercero que esté contratado en relación con dichas políticas, y cualquier proceso que tengan en marcha para auditar a los proveedores externos que prestan servicios de gestión de riesgos de ciberseguridad.
- **Revelar cualquier riesgo, incluidos los incidentes de ciberseguridad anteriores** que les hayan afectado materialmente o que sea razonablemente probable que les afecten.
- **Describir los procesos de sus consejos de administración para la supervisión de los riesgos de ciberseguridad** y los procesos mediante los cuales se informa a los consejos de administración de dichos riesgos, incluido el papel de la dirección en la evaluación y gestión de los riesgos cibernéticos. Las organizaciones, sin embargo, no están obligadas a revelar la experiencia en ciberseguridad representada en sus consejos.

La norma también exige a los emisores privados extranjeros que realicen divulgaciones similares.

Gestión de riesgos cibernéticos de forma más eficaz

Los nuevos requerimientos entrarán en vigor en diciembre de 2023, y las empresas más pequeñas tendrán hasta junio de 2024 para empezar a cumplirlos. La norma destaca la importancia de que todas las empresas públicas dispongan de sólidos marcos de gestión de riesgos de ciberseguridad. A la luz de la nueva norma de la SEC, las empresas deben considerar la implementación de los siguientes procesos de mitigación de riesgos cibernéticos:

1. **Respuesta a incidentes y planificación de la continuidad del negocio.** Las organizaciones deben revisar y modificar los planes existentes de respuesta a incidentes y continuidad del negocio y tener en cuenta los requisitos de tiempo y divulgación. Si aún no disponen de tales planes, ahora sería un buen momento para crearlos. Es esencial poner a prueba estos planes, ya sean de nueva creación o simplemente actualizados a la luz de la nueva norma de la SEC.

2. **Análisis de la postura de seguridad.** Las organizaciones deberían:
   - Examinar sus prácticas de manejo de datos y revisarlas para garantizar los mejores protocolos de tratamiento de datos.
   - Revisar y evaluar los programas de gestión de proveedores externos, incluida la realización de evaluaciones de riesgos de proveedores.
   - Establecer buenas prácticas de higiene cibernética, incluida la supervisión periódica de los controles de seguridad, así como la planificación y presupuestación de mejoras de la seguridad de la información.

3. **Políticas de gobernanza.** Las organizaciones deben evaluar las políticas existentes en materia de gestión de riesgos de ciberseguridad y su supervisión. Y aunque la nueva norma no exige que los expertos en ciberseguridad estén incluidos en los consejos de administración, las empresas públicas deben considerar si dicha experiencia es necesaria para apoyar sus evaluaciones y gobernanza.

Consideraciones adicionales sobre los riesgos de las empresas públicas

Además de tomar medidas para gestionar mejor los riesgos de ciberseguridad y cumplir con la nueva norma de la SEC, las empresas públicas también deben ser conscientes de la posibilidad tanto de litigios de los accionistas como de investigaciones y procedimientos de la SEC en caso de incumplimiento.

El cumplimiento puede ser un reto para algunas empresas, que pueden no estar aún listas en diciembre de, entre otras cosas, describir sus procesos para identificar y gestionar las amenazas de ciberseguridad.

También podrían surgir litigios contra las empresas a las que les resulte difícil cumplir el breve plazo de cuatro días para notificar incidentes tras la determinación de su materialidad. Incluso si un incidente se considera material y se notifica en el plazo de cuatro días, podría resultar difícil para las empresas proporcionar los detalles requeridos o hacer declaraciones que más tarde resulten ser incompletas o inexactas.

Además, los litigios podrían incluir alegaciones de declaraciones falsas sobre:

- Los procesos de las empresas para evaluar, identificar y gestionar los riesgos materiales derivados de las amenazas a la ciberseguridad.
- La supervisión por parte de los consejos de administración de los riesgos relacionados con la ciberseguridad y el papel y la experiencia de la dirección en la evaluación y gestión de los riesgos materiales derivados de las amenazas cibernéticas.

Tanto los litigios de los accionistas como las investigaciones de la SEC podrían resultar costosas para las empresas y los miembros individuales de los consejos de administración. Los accionistas parecen más dispuestos que nunca a encontrar razones para presentar demandas alegando mala gestión empresarial e incumplimiento de los deberes fiduciarios a raíz de cualquier acontecimiento adverso, especialmente si el precio de las acciones de una empresa se ve afectado. La SEC también se ha mostrado especialmente agresiva últimamente.

Un enfoque coordinado

A la luz de los nuevos requisitos, es vital que las empresas públicas trabajen con asesores jurídicos, técnicos y de seguros para comprender sus posibles riesgos y crear marcos para cumplir con los requerimientos de la SEC.

En la medida en que las empresas públicas deseen transferir el riesgo a las pólizas de seguros, deben asegurarse de que esas pólizas -incluidos los seguros de Cyber y D&O (Directores & Funcionarios) y posiblemente otras formas de cobertura- estén bien coordinadas. También deben trabajar con sus asesores de seguros para asegurarse de que tienen sumas aseguradas suficientes y que el lenguaje de la póliza cumple con sus expectativas de cobertura.

CONTACTO

Ricardo Millán
Head Professional & Financial Risks - ProFin

ricardo.millan@lockton.com

LOCKTON®

UNCOMMONLY INDEPENDENT

 |