TONE at the TOP®

Proporcionar a la alta dirección, juntas directivas y comités de auditoría, información concisa sobre temas relacionados con la gobernanza.

Edición 119 | Octubre 2023

Nuevas Reglas de Divulgación de Ciberseguridad de la SEC: *¿Qué deben hacer las Juntas Directivas para estar al día?*

Las nuevas reglas de divulgación de ciberseguridad de la Comisión de Bolsa de Valores de EE. UU. elevan aún más la importancia de una gobernanza vigorosa sobre este riesgo omnipresente. Dada la reciente finalización de las reglas, "las empresas que cotizan en bolsa de todos los tamaños están ahora en una carrera para cumplir antes de los plazos especificados, que se avecinan", señaló un artículo de la NACD.[1] Comprender los impactos de las nuevas reglas y tomar medidas para garantizar el cumplimiento debe ser una máxima prioridad para las organizaciones. Esta edición de "Tone at the Top" examina las nuevas directivas y analiza las contribuciones clave que la auditoría interna puede hacer en los esfuerzos de ciberseguridad de una empresa. También destaca nuevas responsabilidades y otras consideraciones importantes para los miembros de la junta.

Una Amenaza Creciente

La ciberseguridad consiste en proteger los recursos de información de una organización, incluidos computadores, dispositivos de red, software y datos, contra el acceso no autorizado, la interrupción o la destrucción. Sin embargo, con cada avance tecnológico, los estafadores encuentran nuevas formas de lanzar ataques de ciberseguridad, lo que hace que el riesgo cibernético sea una consideración importante para cualquier empresa.

Los costos de las infracciones cibernéticas pueden ser devastadores: casi el 60% de los líderes de ciberseguridad del sector privado que respondieron a un estudio de Cisco informaron haber experimentado un incidente de ciber seguridad en los últimos 12 meses, y para el 41% de los afectados el costo fue de al menos $500,000.[2] Además de los costos financieros directos, los delitos y ataques cibernéticos pueden impedir la capacidad de una empresa para hacer negocios, exponer datos corporativos y de clientes confidenciales y dañar su reputación

No es ninguna sorpresa, entonces, que el verano pasado la SEC emitiera nuevas reglas sobre cómo las empresas que cotizan en bolsa deben informar violaciones importantes de ciberseguridad y revelar información sobre su gestión de riesgos de ciberseguridad, estrategia y prácticas de gobernanza. La regla actualiza y finaliza las propuestas que fueron emitidas en 2022.

El Impacto del Riesgo Cibernético

¿Qué consecuencias negativas han enfrentado las organizaciones debido a ciber incidentes y brechas?

Impacto	2021 RANGO	2023 RANGO	2023 PORCENTAJE
Interrupción operativa (incluida la cadena de suministro o el ecosistema de socios)	1	1	58%
Pérdida de ingresos	9	2	56%
Pérdida de confianza del cliente / impacto negativo de la marca	4	3	56%
Pérdida de Reputación	5	4	55%
Desfinanciamiento de una iniciativa estratégica	N/A	5	55%
Pérdida de confianza en la integridad tecnológica	N/A	6	55%
Impacto negativo en el reclutamiento/retención del talento humano	8	7	54%
Robo de propiedad intelectual	2	8	54%
Caída del precio de las acciones	2	9	52%
Multas Regultorias	7	10	52%
Cambio de Liderazgo	5	N/A	N/A

Fuente: 2023 Global Future of Cyber Survey, Deloitte, 2023

Nota: Basado en la frecuencia de la clasificación de los dos primeros en 2021, selección de los dos primeros puestos en 2023

Acerca del IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin fines de lucro que presta servicios a más de 230.000 miembros globales y ha otorgado 185.000 certificaciones de Auditor Interno (CIA) en todo el mundo. Fundado en 1941, el IIA es reconocido a nivel global como el líder de la profesión de auditoria interna en estándares, certificaciones, educación, investigación y orientación técnica. Para obtener más información, visite theiia.org.

El IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

Suscripciones Gratuitas

Visite theiia.org/Tone para registrarse..

Ampliación de la Divulgación sobre Gestión e Incidentes de Ciberseguridad.

Las reglas de la SEC tienen como objetivo mejorar y estandarizar las divulgaciones de ciberseguridad por parte de empresas públicas sujetas a los requisitos de presentación de informes de la Ley de Bolsa de Valores. Las nuevas reglas mejoran lo que las empresas deben informar en relación con la gestión de riesgos, la estrategia, la gobernanza y los incidentes de ciberseguridad que se consideran materiales. Las nuevas reglas incluyen:

- Describir cómo evalúan, identifican y gestionan las amenazas a la ciberseguridad y si algún riesgo ha afectado materialmente o es razonablemente probable que afecte materialmente su estrategia comercial, resultados de operaciones o situación financiera. También deben divulgar incidentes materiales de ciberseguridad y describir los aspectos materiales de la naturaleza, alcance y momento de cada incidente.

- Detallar cómo la junta supervisa los riesgos cibernéticos y el papel de la administración en la evaluación y gestión de riesgos materiales. La SEC decidió no adoptar un requisito propuesto sobre la divulgación de la experiencia de la junta en ciberseguridad.

- Los emisores privados extranjeros están sujetos a las mismas reglas y también deben proporcionar información sobre incidentes importantes de ciberseguridad que cometan o estén obligados a hacer públicos o divulgar de otro modo en una jurisdicción extranjera, a cualquier bolsa de valores o a los tenedores de valores.

- Presentar un Formulario 8-K generalmente dentro de los cuatro días hábiles posteriores a que una organización determine que un incidente cibernético es material. (Se pueden permitir retrasos en la divulgación si el Fiscal General de los Estados Unidos determina que la divulgación inmediata representaría un riesgo sustancial para la seguridad nacional o la seguridad pública y notifica a la SEC por escrito).

Consideraciones Clave para las Juntas Directivas

Muchas organizaciones están realizando evaluaciones de brechas para comprender qué tan bien están identificando, analizando, gestionando y recuperándose actualmente de eventos cibernéticos. Dadas las nuevas reglas, las juntas deben asegurarse de que la administración esté determinando si el proceso de evaluación existente respaldará un cambio de cuatro días, dijo George Barham, CIA, CRMA, CISA, Director de Estándares y Orientación Profesional del Instituto de Auditores Internos (IIA). Y si bien el equipo de TI identificará los incidentes, la determinación de la materialidad debe incluir aportes de otras áreas, como los equipos financiero, legal y regulatorio, para obtener una perspectiva amplia.

Los miembros de la junta también deben ser conscientes de que la materialidad tiene elementos tanto cuantitativos como cualitativos. "Se trata de algo más que el impacto del dólar", dijo Barham. También implica consideraciones legales y regulatorias. Si la empresa opera en la Unión Europea, por ejemplo, un incidente puede estar sujeto al Reglamento General de Protección de Datos (GDPR). Las consideraciones estratégicas también pueden ser un factor de materialidad si, por ejemplo, el incidente implicó la exposición de secretos comerciales u otra información que le dé a la organización una ventaja competitiva. La determinación de materialidad debe incluir cualquier consideración que pueda tener un impacto en el análisis de la empresa por parte de un inversor, dijo Barham.

Debido a que el Artículo 106 del Reglamento aborda las funciones y responsabilidades de la junta, el 10-K anual es el lugar donde las organizaciones deben documentar su gobernanza de la ciberseguridad. Podría informar, por ejemplo, que el comité de auditoría de la junta directiva es responsable de revisar el riesgo cibernético, lo que suele ser el caso, y también podría cubrir cómo la administración informa al comité de auditoría o a la junta sobre cuestiones de ciberseguridad. Como parte de las responsabilidades de los miembros de la junta directiva, deben comprender las calificaciones de quién aborda las cuestiones de ciberseguridad a nivel gerencial y cómo se gestionan y mitigan las ciberamenazas.

La Contribución de la Auditoría Interna

Los auditores internos suelen ser responsables de identificar y probar controles internos clave que ayudan a mitigar los riesgos relacionados con la ciberseguridad, incluida la referencia a marcos de control ampliamente adoptados. A la luz de las nuevas reglas, los órganos de gobierno y la alta dirección de las organizaciones necesitarán garantías independientes, objetivas y bien informadas para validar la eficacia y eficiencia de los controles de recuperación y respuesta de ciberseguridad. La auditoría interna puede proporcionar esta garantía de conformidad con sus propios estándares profesionales, así como con marcos de control ampliamente aceptados, particularmente aquellos utilizados por las funciones de seguridad de la información y TI de la organización. Los auditores internos también pueden ofrecer servicios de aseguramiento para que las empresas determinen la mejor manera de protegerse contra los riesgos cibernéticos.

A medida que las organizaciones determinan cómo abordar los nuevos requisitos, algunas funciones específicas para el director ejecutivo de auditoría y el equipo de auditoría interna pueden incluir:

- Consultar con las juntas directivas, la dirección ejecutiva y los líderes de gestión de riesgos de ciberseguridad sobre el impacto esperado de las reglas desde las perspectivas del plan financiero, de planificación estratégica, de cumplimiento y de auditoría.
- Actualizar las evaluaciones de riesgos con respecto al cumplimiento de las nuevas regulaciones y apoyar los preparativos de la organización para cumplir con los requisitos. Si la auditoría interna aún no participa en las evaluaciones de riesgos de ciberseguridad, podría comenzar a contribuir a este proceso.
- Informar sobre si los controles de ciberseguridad actuales están diseñados de manera adecuada y operan de manera efectiva para que la organización cumpla con las nuevas reglas.

"La ciberseguridad suele considerarse una de las áreas de mayor riesgo que las organizaciones deben gestionar", señaló Barham, por lo que ciertamente ya está en el radar de la auditoría interna. Eso significa que auditoría interna es consciente de los riesgos relacionados y de los controles internos necesarios para mitigarlos. La auditoría interna también puede proporcionar la información y los conocimientos que las juntas necesitan para cumplir con sus responsabilidades de gobernanza de la ciberseguridad según las nuevas reglas. Además de la perspectiva que brinda la administración, la auditoría interna puede ofrecer un punto de vista independiente y objetivo sobre cómo se gestionan y divulgan los riesgos cibernéticos. Puede asesorar al comité de auditoría sobre la incorporación de riesgos y regulaciones de ciberseguridad en el plan de auditoría e informar sobre qué tan bien se está preparando la organización para cumplir con las reglas de la SEC y qué tan bien las implementa en el futuro.

Cumplir la Fecha Límite

Para las divulgaciones de incidentes, o Formularios 8-K, las reglas entran en vigencia 90 días después de su publicación en el Registro Federal o el 18 de diciembre de 2023 (las empresas informantes más pequeñas tienen hasta 180 días adicionales para cumplir). Las divulgaciones del Formulario 10-K deberán presentarse a partir de los informes anuales de los años fiscales que finalicen a partir del 15 de diciembre de 2023. La NACD señaló que, aunque las nuevas reglas no abordan las calificaciones de los miembros de la junta, éstas "elevan el papel de todos los líderes, incluidos la junta, los directores ejecutivos y los directores de seguridad de la información, en la gestión de riesgos". A medida que los miembros de la junta directiva abordan sus nuevas responsabilidades, pueden recurrir a auditoría interna para obtener el valioso aseguramiento y conocimiento que necesitarán para abordar los problemas de ciberseguridad.

PREGUNTAS PARA MIEMBROS DE LA JUNTA

- ¿Cómo garantiza la organización que estará preparada para cumplir con las nuevas reglas de la SEC?
- ¿Qué tipos de controles existen ya para prevenir o mitigar los ciberataques? ¿Qué tan exitosos han sido?
- ¿Se están implementando nuevos controles o procedimientos de presentación de informes para abordar las nuevas reglas de la SEC? Si es así, ¿cuáles son?
- ¿Ha experimentado la organización algún incidente cibernético importante en los últimos dos años? ¿Cómo se abordaron y qué mejoras se podrían hacer?
- ¿Qué tipo de aseguramiento de auditoría o asesoramiento de auditoría interna puede ayudar a la junta a cumplir con sus responsabilidades de supervisión del riesgo cibernético?

"Time Is of the Essence with SEC's Approved Cybersecurity Disclosure Rules," James Turgal, NACD, September 12, 2023.
Cisco Cyber Security Readiness Index: Resilience in a Hybrid World Cisco, March 2023.