La SEC propone la regla del agente de bolsa, que aborda los riesgos de ciberseguridad, con XML personalizado





Publicado el miércoles, 15 de marzo de 2023

La Comisión de Bolsa y Valores (SEC) publicó una propuesta de regla, Addressing Cybersecurity Risks to the U.S. Securities Markets, que exige que los corredores de bolsa, la Junta Municipal de Reglamentación de Valores, las agencias de compensación, los principales participantes de swaps basados en valores, las asociaciones y bolsas nacionales de valores, los repositorios de datos de swaps basados en la seguridad y los agentes de intercambio, y los agentes de transferencia, aborden sus riesgos de ciberseguridad. Se les pedirá que adopten políticas y procedimientos y, en caso de un incidente significativo de ciberseguridad, informen a la SEC en el Formulario SCIR propuesto. Además, estas entidades tendrían que divulgar públicamente descripciones resumidas de sus riesgos e incidentes de ciberseguridad. La regla exige que Form SCIR se prepare mediante un esquema XML personalizado.

Lea la [propuesta.](https://www.sec.gov/rules/proposed/2023/34-97142.pdf)

Lea la [hoja informativa.](https://www.sec.gov/files/34-97142-fact-sheet.pdf)

[CORREDORES DE BOLSA](https://xbrl.us/home/tag/broker-dealers/)



Abordar los riesgos de ciberseguridad para los mercados de valores de EE. UU.

La Comisión de Bolsa y Valores propuso una nueva regla, forma y enmiendas relacionadas para exigir que las entidades que realizan servicios críticos respalden las operaciones justas, ordenadas y eficientes de los mercados de valores de los Estados Unidos aborden sus riesgos de ciberseguridad. Los nuevos requisitos se aplicarían a los corredores de bolsa, la Junta Municipal de Reglamentación de Valores, las agencias de compensación, los principales participantes en swaps basados en valores, las asociaciones nacionales de valores, las bolsas nacionales de valores, los repositorios de datos de swaps basados en valores, los agentes de swaps basados en valores y los agentes de transferencia (colectivamente, "Entidades de Mercado").

Por qué esto es importante

Los mercados de valores de los Estados Unidos forman parte del Sector de Servicios Financieros, uno de los dieciséis sectores de infraestructura crítica "cuyos activos, sistemas y redes, ya sean físicos o virtuales, se consideran tan vitales para los Estados Unidos que su incapacitación o destrucción tendría un efecto debilitante en la seguridad, la seguridad económica nacional, la salud o seguridad pública nacional, o cualquier combinación de los mismos. " según la Agencia de Seguridad de Ciberseguridad e Infraestructura. El sector de servicios financieros está siendo atacado cada vez más por actores de amenazas cibernéticas que utilizan tácticas, técnicas y procedimientos sofisticados y en constante evolución para causar incidentes de ciberseguridad dañinos. Esto plantea un grave riesgo para los mercados de valores de Estados Unidos. La propuesta está diseñada para abordar y mitigar este riesgo exigiendo a las entidades del mercado que tomen medidas para protegerse a sí mismas y a los inversores de los impactos dañinos de los incidentes de ciberseguridad.

Cómo se aplicaría esta nueva regla y forma

La nueva Regla 10 propuesta requeriría que todas las Entidades del Mercado establezcan, mantengan y hagan cumplir políticas y procedimientos escritos que estén razonablemente diseñados para abordar sus riesgos de ciberseguridad. Todas las entidades del mercado también deberían, al menos una vez al año, revisar y evaluar el diseño y la eficacia de sus políticas y procedimientos de ciberseguridad, incluso si reflejan cambios en el riesgo de ciberseguridad durante el período cubierto por la revisión. Todas las entidades del mercado también tendrían que notificar por escrito a la Comisión de inmediato un incidente significativo de ciberseguridad cuando dispongan de una base razonable para concluir que el incidente significativo de ciberseguridad se ha producido o se está produciendo.

Las entidades del mercado, que no sean ciertos tipos de pequeños corredores de bolsa, estarían sujetas a requisitos adicionales en virtud de la nueva Regla 10 propuesta como "Entidades cubiertas".

En primer lugar, la regla propuesta requeriría que las Entidades Cubiertas adopten políticas y procedimientos para abordar los riesgos de ciberseguridad que tendrían que incluir específicamente lo siguiente:

• Evaluaciones periódicas de los riesgos de ciberseguridad asociados con los sistemas de información de la Entidad Cubierta y documentación escrita de las evaluaciones de riesgos;

• Controles diseñados para minimizar los riesgos relacionados con el usuario y evitar el acceso no autorizado a los sistemas de información de la Entidad Cubierta;

• Medidas diseñadas para monitorear los sistemas de información de la Entidad Cubierta y proteger la información de la Entidad Cubierta del acceso o uso no autorizado, y supervisar a los proveedores de servicios que reciben, mantienen o procesan información o que de otra manera tienen permiso para acceder a los sistemas de información de la Entidad Cubierta;

• Medidas para detectar, mitigar y remediar cualquier amenaza y vulnerabilidad de ciberseguridad con respecto a los sistemas de información de la Entidad Cubierta; y

• Medidas para detectar, responder y recuperarse de un incidente de ciberseguridad y procedimientos para crear documentación escrita de cualquier incidente de ciberseguridad y la respuesta y recuperación del incidente.

En segundo lugar, después de proporcionar un aviso electrónico inmediato por escrito de un incidente significativo de ciberseguridad, las entidades cubiertas tendrían que informar a la Comisión y actualizar la información sobre el incidente de ciberseguridad significativo mediante la presentación de la Parte I del formulario SCIR propuesto. El formulario obtendría información sobre el incidente de ciberseguridad significativo y los esfuerzos de la Entidad Cubierta para responder y recuperarse del incidente.

En tercer lugar, la propuesta requeriría que las Entidades Cubiertas divulguen públicamente descripciones resumidas de sus riesgos de ciberseguridad y los incidentes significativos de ciberseguridad que experimentaron durante el año calendario actual o anterior en la Parte II del Formulario SCIR propuesto. Una entidad cubierta tendría que presentar el formulario ante la Comisión y publicarlo en su sitio web. Las Entidades Cubiertas que llevan o introducen corredores de bolsa también tendrían que proporcionar el formulario a los clientes en la apertura de la cuenta, cuando se actualice la información en el formulario, y anualmente.

Información adicional:

El período de comentarios públicos permanecerá abierto hasta 60 días después de la fecha de publicación de la publicación propuesta en el Registro Federal.



Regla de gestión de riesgos de ciberseguridad para corredores de bolsa, agencias de compensación, principales participantes de swaps basados en seguridad, la Junta Municipal de Reglamentación de Valores, asociaciones nacionales de valores, bolsas nacionales de valores, repositorios de datos de swaps basados en valores, agentes de swaps basados en seguridad y agentes de transferencia

AGENCIA: Comisión de Bolsa y Valores.

ACCIÓN: Norma propuesta.

RESUMEN: La Comisión de Bolsa y Valores ("Comisión") propone una nueva regla y forma y enmiendas a las reglas existentes de mantenimiento de registros para exigir a los corredores de bolsa, agencias de compensación, principales participantes de swaps basados en valores, la Junta Municipal de Reglamentación de Valores, asociaciones nacionales de valores, bolsas nacionales de valores, repositorios de datos de swaps basados en valores, agentes de swaps basados en valores y agentes de transferencia para abordar los riesgos de ciberseguridad a través de políticas y procedimientos, notificación inmediata a la Comisión de la ocurrencia de un incidente significativo de ciberseguridad y, según corresponda, notificación detallada a la Comisión sobre un incidente significativo de ciberseguridad, y revelaciones públicas que mejoren la transparencia con respecto a los riesgos de ciberseguridad y los incidentes significativos de ciberseguridad. Además, la Comisión propone enmiendas a las órdenes de exención existentes de los organismos de compensación para exigir la conservación de los registros que tendrían que realizarse en virtud de los requisitos de ciberseguridad propuestos. Por último, la Comisión propone modificaciones para abordar la posible disponibilidad de los operadores de swaps basados en valores y de los principales participantes en swaps basados en valores de cumplimiento sustituido en relación con dichos requisitos.

FECHAS: Los comentarios deben recibirse a más tardar el 5 de junio de 2023.

DIRECCIONES: Los comentarios pueden enviarse por cualquiera de los siguientes métodos:

**Comentarios electrónicos:**

• Utilice el formulario de comentarios de la Comisión en Internet (<https://www.sec.gov/rules/submitcomments.htm>); o

• Envíe un correo electrónico a rule-comments@sec.gov. Por favor, incluya el número de expediente S7-06-23 en la línea de asunto.

**Comentarios del artículo:**

• Envíe comentarios en papel al secretario, Comisión de Bolsa y Valores, 100 F Street, NE, Washington, DC 20549-1090.

Todas las presentaciones deben referirse al número de expediente S7-06-23. El número de archivo debe incluirse en la línea de asunto si se utiliza el correo electrónico. Para ayudar a la Comisión a procesar y revisar sus comentarios de manera más eficiente, utilice solo un método de presentación. La Comisión publicará todos los comentarios en el sitio web de la Comisión (https://www.sec.gov/rules/proposed.shtml). Los comentarios también están disponibles para su visualización e impresión en el sitio web en la Sala de Referencia Pública de la Comisión, 100 F Street, NE, Washington, DC 20549, en días hábiles oficiales entre las 10 a.m. y las 3 p.m. Las condiciones de funcionamiento pueden limitar el acceso a la sala de referencia pública de la Comisión. Todos los comentarios recibidos se publicarán sin cambios; la Comisión no edita la información de identificación personal de las presentaciones. Debe enviar solo la información que desea poner a disposición del público.

La Comisión o el personal pueden agregar estudios, memorandos u otros elementos sustantivos al archivo de comentarios durante esta reglamentación. Una notificación de la inclusión en el archivo de comentarios de dichos materiales estará disponible en el sitio web de la Comisión. Para garantizar la recepción electrónica directa de dichas notificaciones, regístrese a través de la opción "Manténgase conectado" en www.sec.gov para recibir notificaciones por correo electrónico.

PARA OBTENER MÁS INFORMACIÓN, PÓNGASE EN CONTACTO CON: Randall W. Roy, Director Asociado Adjunto y Nina Kostyukovsky, Asesora Especial, Oficina de Finanzas de Corredores de Bolsa (con respecto a la regla y forma de ciberseguridad propuesta y los aspectos de la propuesta exclusivos de los corredores de bolsa); Matthew Lee, Subdirector y Stephanie Park, Asesora Especial Superior, Oficina de Compensación y Liquidación (con respecto a aspectos de la propuesta exclusivos de los organismos de compensación y los repositorios de datos de intercambio basados en valores); John Guidroz, Director Adjunto y Russell Mancuso, Asesor Especial de la Oficina de Política de Derivados (con respecto a los aspectos de la propuesta exclusivos de los principales participantes en swaps basados en valores y operadores de swaps basados en valores); Michael E. Coe, Subdirector y Leah Mesfin, Asesora Especial, Oficina de Supervisión del Mercado (con respecto a aspectos de la propuesta exclusivos de las asociaciones nacionales de valores y las bolsas nacionales de valores); Moshe Rothman, Subdirector, Oficina de Compensación y Liquidación (con respecto a aspectos de la propuesta exclusivos de los agentes de transferencia) en (202) 551-5500, División de Comercio y Mercados; y Dave Sánchez, Director, Adam Wendell, Director Adjunto, y Adam Allogramento, Asesor Especial, Oficina de Valores Municipales (con respecto a aspectos de la propuesta exclusivos de la Junta de Reglamentación de Valores Municipales) al (202) 551-5680, Comisión de Bolsa y Valores, 100 F Street NE, Washington, DC 20549-7010.

INFORMACIÓN COMPLEMENTARIA: La Comisión propone añadir la siguiente nueva norma y forma en virtud de la Ley del Mercado de Valores de 1934 ("Ley de Bolsa"): (1) 17 CFR 242.10 ("Regla 10"); y (2) 17 CFR 249.642 ("Formulario SCIR"). La Comisión también propone enmiendas conexas a las siguientes normas: 1) 17 CFR 232.101; (2) 17 CFR 240.3a71-6; (3) 17 CFR 240.17a-4; (4) 17 CFR 240.17Ad-7; (5) 17 CFR 240.18a-6; y (6) 17 CFR 240.18a-10. Además, la Comisión propone modificar determinadas órdenes que eximen del registro a las agencias compensadoras.



I. INTRODUCCIÓN

A. El riesgo de ciberseguridad representa una amenaza para los mercados de valores de Estados Unidos

1. En general

El riesgo de ciberseguridad se ha descrito como "un efecto de la incertidumbre en o dentro de la información y la tecnología". Este riesgo puede conducir a "la pérdida de confidencialidad, integridad o disponibilidad de información, datos o sistemas de información (o control) y [por lo tanto] posibles impactos adversos a las operaciones de la organización (es decir, misión, funciones, imagen o reputación) y activos, individuos, otras organizaciones y la nación". El Consejo de Supervisión de Estabilidad Financiera de los Estados Unidos ("FSOC") en su informe anual de 2021 declaró que un incidente de ciberseguridad desestabilizador podría amenazar la estabilidad del sistema financiero de los Estados Unidos a través de al menos tres canales:

• En primer lugar, el incidente podría interrumpir un servicio financiero clave o una utilidad para la que hay poco o ningún sustituto. Esto podría incluir ataques a los bancos centrales; Intercambios; acreedores soberanos y subsoberanos, incluidos los gobiernos estatales y locales de los Estados Unidos; bancos custodios; sistemas de compensación y liquidación de pagos; u otras empresas o servicios que carezcan de sustitutos o sean proveedores exclusivos de servicios.

• En segundo lugar, el incidente podría comprometer la integridad de los datos críticos. La información precisa y utilizable es fundamental para el funcionamiento estable de las empresas financieras y del sistema; Si dichos datos se corrompen a una escala suficientemente grande, podrían interrumpir el funcionamiento del sistema. La pérdida de dichos datos también tiene implicaciones de privacidad para los consumidores y podría conducir al robo de identidad y al fraude, lo que a su vez podría resultar en una pérdida de confianza.

• En tercer lugar, un incidente de ciberseguridad que cause una pérdida de confianza entre un amplio conjunto de clientes o participantes del mercado podría hacer que los clientes o participantes cuestionen la seguridad o liquidez de sus activos o transacciones, y conducir a una retirada significativa de activos o actividades.

Los mercados de valores de los Estados Unidos son parte del Sector de Servicios Financieros, uno de los dieciséis sectores de infraestructura crítica "cuyos activos, sistemas y redes, ya sean físicos o virtuales, se consideran tan vitales para los Estados Unidos que su incapacitación o destrucción tendría un efecto debilitante en la seguridad, la seguridad económica nacional, la salud o seguridad pública nacional, o cualquier combinación de los mismos". Estos mercados tienen más de $ 100 billones en tamaño total, y más de un billón de dólares en transacciones fluyen a través de ellos cada día. Por ejemplo, la capitalización de mercado del mercado de acciones de EE.UU. se valoró en 49 billones de dólares a partir del primer trimestre de 2022, y a partir de mayo de 2022, el volumen diario promedio de negociación en dólares en el mercado de acciones de EE.UU. fue de 659.000 millones de dólares. La capitalización de mercado del mercado de renta fija de EE.UU. se valoró en 52,9 billones de dólares a partir del cuarto trimestre de 2021, y a partir de mayo de 2022, el volumen medio diario de negociación en dólares en el mercado de renta fija de EE.UU. fue de 897.800 millones de dólares.

El tamaño de estos mercados es indicativo del papel central que desempeñan en la economía estadounidense en términos del flujo de capital, incluidos los ahorros de los inversores individuales que dependen cada vez más de ellos para, por ejemplo, generar riqueza para financiar su jubilación, comprar una casa o pagar la universidad para ellos o su familia. Por lo tanto, es de vital importancia para la economía, los inversores y la formación de capital de los Estados Unidos que los mercados de valores de los Estados Unidos funcionen de manera justa, ordenada y eficiente.

El funcionamiento justo, ordenado y eficiente de los mercados de valores de los Estados Unidos depende de diferentes tipos de entidades que realizan diversas funciones para apoyar, entre otras cosas, la difusión de información sobre el mercado, la suscripción de emisiones de valores, la creación de mercados de valores, la negociación de valores, el suministro de liquidez a los mercados de valores, la ejecución de transacciones de valores, la compensación y liquidación de transacciones de valores, la financiación de transacciones de valores, el registro y la transferencia de valores. la propiedad, el mantenimiento de la custodia de valores, el pago de dividendos e intereses sobre valores, el reembolso del principal de las inversiones en valores, la supervisión de los participantes regulados del mercado y el seguimiento de las actividades del mercado. En conjunto, estas funciones son desempeñadas por entidades reguladas por la Comisión: corredores de bolsa, corredores de bolsa que operan un sistema de negociación alternativo ("ATS"), agencias de compensación, principales participantes en swaps basados en valores ("MSBSP"), la Junta Municipal de Reglamentación de Valores ("MSRB"), asociaciones nacionales de valores, bolsas nacionales de valores, repositorios de datos de swaps basados en valores ("SBSDR"), agentes de swaps basados en valores ("SBSD" o colectivamente con MSBSP, "Entidades SBS"), y transferencias, agentes (colectivamente, "Entidades de Mercado").

Para realizar sus funciones, las Entidades del Mercado se basan en una serie de sistemas electrónicos de información, comunicación e informática (o sistemas similares) ("sistemas de información") y redes de sistemas de información interconectados. Si bien las entidades del mercado han confiado durante mucho tiempo en los sistemas de información para realizar sus diversas funciones, la aceleración de la innovación técnica en los últimos años ha ampliado exponencialmente el papel que desempeñan estos sistemas en los mercados de valores de los Estados Unidos. Esta expansión ha sido impulsada por las mayores eficiencias y menores costos que se pueden lograr mediante el uso de sistemas de información. También ha sido impulsado por nuevos participantes (empresas de tecnología financiera (Fintech)) que han desarrollado modelos de negocio que dependen en gran medida de los sistemas de información (por ejemplo, aplicaciones en dispositivos móviles) para proporcionar servicios a los inversores y otros participantes en los mercados de valores y entidades de mercado más establecidas que adoptan el uso de tecnologías similares. La pandemia de COVID-19 también ha contribuido a una mayor dependencia de los sistemas de información.

Esta mayor dependencia de los sistemas de información por parte de las Entidades del Mercado ha provocado un aumento correspondiente en su riesgo de ciberseguridad. Este riesgo puede ser causado por las acciones de actores de amenazas externas, incluidos actores de amenazas organizadas o individuales que buscan ganancias financieras, estados nacionales que realizan operaciones de espionaje o individuos que protestan, actúan con rencores u ofensas personales, o buscan emociones.16 Los actores de amenazas internas (por ejemplo, empleados descontentos o empleados que buscan ganancias financieras) también pueden ser fuentes de riesgo de ciberseguridad. Los actores de amenazas pueden dirigirse a las entidades del mercado porque manejan activos financieros o información patentada sobre activos y transacciones financieras. Además de los actores de amenazas, los errores de los empleados, proveedores de servicios o socios comerciales pueden crear riesgos de ciberseguridad (por ejemplo, exponer erróneamente información confidencial o personal, por ejemplo, enviándola a través de un correo electrónico no cifrado a destinatarios no deseados).

Otro factor que aumenta el riesgo de ciberseguridad para las entidades de mercado es la creciente sofisticación de las tácticas, técnicas y procedimientos empleados por los actores de amenazas. Esta tendencia se ve exacerbada por la capacidad de los actores de amenazas para comprar herramientas para participar en el delito cibernético.

Los actores de amenazas emplean una serie de tácticas para causar incidentes dañinos de ciberseguridad. Una táctica es el uso de software malicioso ("malware") que se carga en un sistema informático y es utilizado por los actores de amenazas para comprometer la confidencialidad de la información almacenada o las operaciones realizadas (por ejemplo, monitoreo de pulsaciones de teclas) en el sistema o la integridad o disponibilidad del sistema (por ejemplo, ataques de comando y control donde un actor de amenazas puede infiltrarse en un sistema para instalar malware que le permita enviar comandos de forma remota a los dispositivos infectados). Hay varias formas diferentes de malware, incluidos adware, botnets, rootkit, spyware, troyanos, virus y gusanos.

Una segunda táctica es una variación del malware conocido como "ransomware". En este esquema, el actor de la amenaza cifra los datos de la víctima haciéndolos inutilizables y luego exige el pago para descifrarlos. Los esquemas de ransomware se han vuelto más frecuentes con la adopción y el uso generalizados de activos criptográficos. Es una táctica común utilizada contra el sector financiero. El personal de la Comisión ha observado que esta táctica se ha empleado cada vez más contra determinadas entidades del mercado.

Otro grupo de tácticas son varios esquemas de ingeniería social. En un ataque de ingeniería social, el actor de amenazas utiliza habilidades sociales para convencer a un individuo de que proporcione acceso o información que se puede utilizar para acceder a un sistema de información. "Phishing" es una variación de un ataque de ingeniería social en el que se utiliza un correo electrónico para convencer a una persona de que proporcione información (por ejemplo, información personal o de cuenta o credenciales de inicio de sesión) que se puede utilizar para obtener acceso no autorizado a un sistema de información. Los actores de amenazas también utilizan sitios web para realizar ataques de phishing. "Spear phishing" es una variación de phishing que se dirige a un individuo o grupo específico. "Vishing" y "smishing" son variaciones de la ingeniería social que utilizan comunicaciones telefónicas o mensajes de texto, respectivamente, para este propósito. Estas tácticas de ingeniería social también se utilizan para engañar al destinatario de una comunicación electrónica (por ejemplo, un correo electrónico o mensaje de texto) para que abra un enlace o archivo adjunto en la comunicación que carga malware en los sistemas de información del destinatario.

Además del malware y la ingeniería social, los actores de amenazas pueden tratar de eludir o frustrar los mecanismos lógicos de seguridad del sistema de información (es decir, "hackear" el sistema). Hay muchas variaciones de hacking. Una táctica es un ataque de "fuerza bruta" en el que el actor de amenazas intenta determinar un valor desconocido (por ejemplo, credenciales de inicio de sesión) utilizando un proceso automatizado que prueba una gran cantidad de valores posibles. El personal de la Comisión ha observado que los agentes amenazantes han empleado cada vez más una variación de esta táctica contra determinadas entidades del mercado para acceder a las cuentas de sus clientes. La capacidad de los actores de amenazas para piratear los sistemas de información puede verse facilitada por vulnerabilidades en los sistemas de información, incluido, por ejemplo, el software que se ejecuta en los sistemas.

Los actores de amenazas también causan incidentes dañinos de ciberseguridad a través de ataques de denegación de servicio ("DoS"). Este tipo de ataque puede involucrar botnets o servidores comprometidos que envían datos o mensajes "basura" a un sistema de información que una Entidad de Mercado utiliza para proporcionar servicios a inversores, participantes del mercado u otras Entidades del Mercado causando que el sistema falle o no pueda procesar las operaciones de manera oportuna. Los ataques DoS son una táctica comúnmente utilizada.

Las tácticas, técnicas y procedimientos empleados por los actores de amenazas pueden afectar los sistemas de información que una entidad de mercado opera directamente (por ejemplo, una aplicación web o un sistema de correo electrónico). También pueden afectar negativamente a la Entidad de Mercado y sus sistemas de información a través de su conexión a sistemas de información operados por terceros, como proveedores de servicios (por ejemplo, proveedores de servicios en la nube), socios comerciales, clientes, contrapartes, miembros, registrantes o usuarios. Además, las tácticas, técnicas y procedimientos empleados por los actores de amenazas pueden afectar negativamente a la Entidad de Mercado y sus sistemas de información a través de su conexión a sistemas de información operados por servicios públicos o plataformas centrales a las que la Entidad de Mercado está conectada (por ejemplo, una bolsa de valores, una plataforma de negociación de valores, una agencia de compensación de valores o un procesador de pagos).

Si el riesgo de ciberseguridad se materializa en un incidente de ciberseguridad significativo, una Entidad de Mercado puede perder su capacidad de realizar una función clave causando daño a la Entidad de Mercado, inversores u otros participantes del mercado. Además, dada la interconexión de los sistemas de información de las entidades de mercado, un incidente significativo de ciberseguridad en una entidad de mercado tiene el potencial de propagarse a otras entidades de mercado en un proceso en cascada que podría causar interrupciones generalizadas que amenacen el funcionamiento justo, ordenado y eficiente de los mercados de valores de los Estados Unidos. Además, la interrupción de una Entidad de Mercado que proporciona servicios críticos a otras Entidades de Mercado a través de sistemas de información conectados podría causar interrupciones en cascada a esas otras Entidades de Mercado en la medida en que no puedan obtener esos servicios críticos de otra fuente.

Un incidente de ciberseguridad significativo también puede resultar en el acceso no autorizado y el uso de información personal, confidencial o patentada. En el caso de la información personal, esto puede causar daños a los inversores y otras personas a cuya información personal se accedió o utilizó (por ejemplo, robo de identidad). Esto podría conducir al robo de activos de los inversores. En el caso de información confidencial o patentada, esto puede causar daño al negocio de la persona a cuya información de propiedad se accedió o utilizó (por ejemplo, exposición pública de posiciones comerciales o estrategias comerciales) o proporcionar al usuario no autorizado una ventaja injusta sobre otros participantes del mercado (por ejemplo, negociación basada en información comercial confidencial). El acceso no autorizado a información patentada también puede conducir al robo de la valiosa propiedad intelectual de una Entidad de Mercado.

Los incidentes de ciberseguridad que afecten a las entidades del mercado pueden causar daños sustanciales a otros participantes del mercado, incluidos los inversores. Por ejemplo, los incidentes significativos de ciberseguridad causados por malware pueden causar la pérdida de los datos de la Entidad de Mercado o de los datos de otros participantes del mercado. Estos incidentes también pueden provocar interrupciones del negocio que no solo son costosas para la Entidad de Mercado, sino también para los otros participantes del mercado que dependen de los servicios de la Entidad de Mercado.

Una entidad de mercado también puede incurrir en costos de remediación sustanciales debido a un incidente significativo de ciberseguridad. Por ejemplo, el incidente puede dar lugar al reembolso a otros participantes del mercado por pérdidas relacionadas con la ciberseguridad y el pago por su uso de servicios de protección de identidad. El hecho de que una entidad de mercado no se proteja adecuadamente contra un incidente significativo de ciberseguridad también puede aumentar sus primas de seguro. Además, un incidente significativo de ciberseguridad puede exponer a una Entidad de Mercado a costos de litigio (por ejemplo, para defender demandas presentadas por personas cuya información personal fue robada), escrutinio regulatorio, daños a la reputación y, si es el resultado de una falla de cumplimiento, sanciones. Finalmente, un incidente de ciberseguridad significativo suficientemente grave podría causar el fracaso de una Entidad de Mercado. Dada la interconexión de las entidades de mercado, un incidente significativo de ciberseguridad que degrade o interrumpa las funciones críticas de una entidad de mercado podría causar daños a otras entidades de mercado (por ejemplo, cortando su acceso a un servicio crítico como la liquidación de valores o exponiéndolas al mismo malware que degradó o interrumpió las funciones críticas de la primera entidad de mercado). Esto podría conducir a interrupciones en todo el mercado que comprometan el funcionamiento justo, ordenado y eficiente de los mercados de valores de los Estados Unidos.

Por estas razones, la Comisión propone nuevos requisitos normativos diseñados para proteger a los mercados de valores estadounidenses y a los inversores en estos mercados de la amenaza que plantean los riesgos de ciberseguridad.