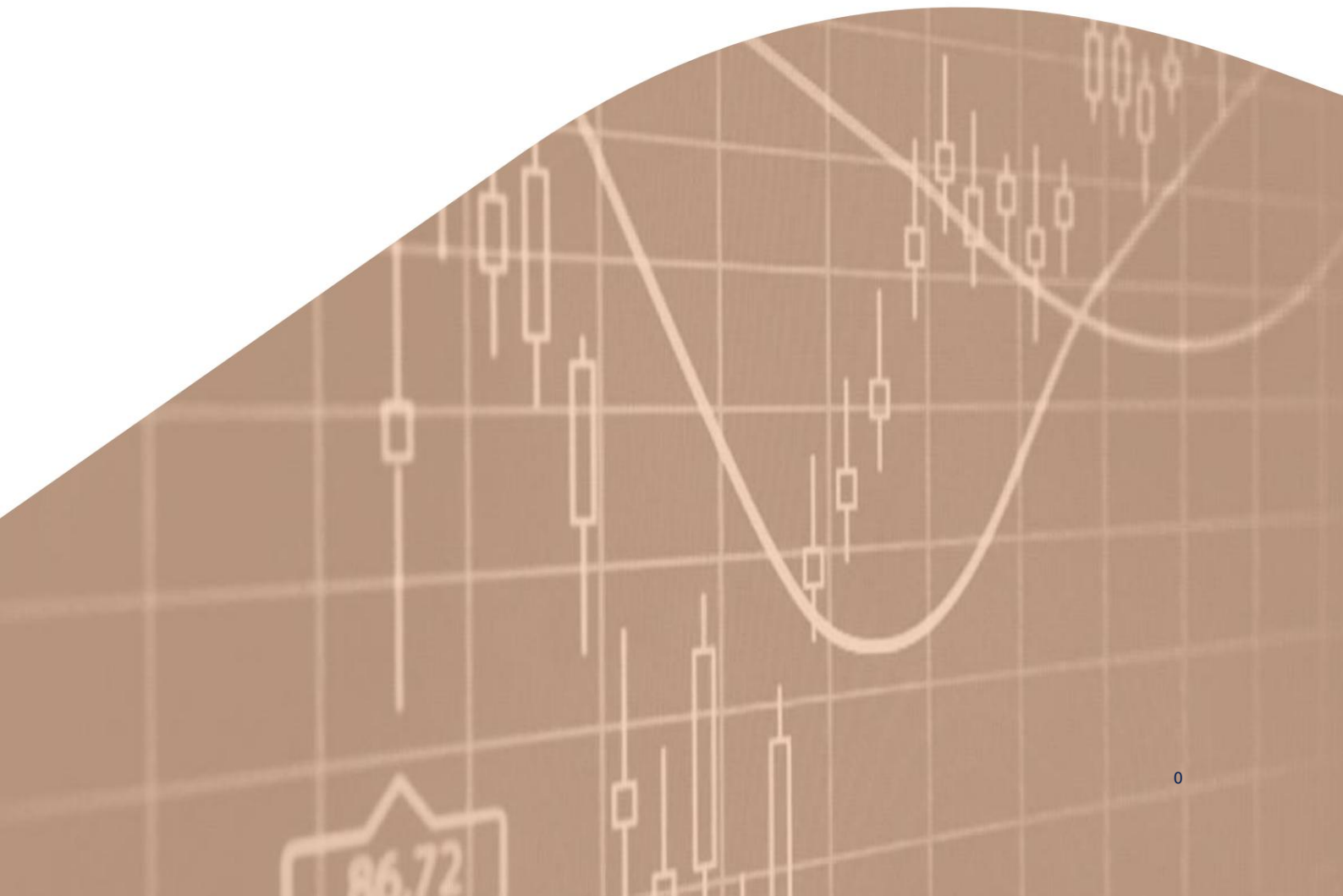
Machine Translated by Google

16 de julio de 2025
ESMA50-1949966494-3823

Análisis de riesgos de TRV de la ESMA

Estabilidad financiera

Riesgos operativos y cibernéticos en Mercados financieros de la UE: medición y simulación de tensiones



Machine Translated by Google

Informe de la ESMA sobre tendencias, riesgos y vulnerabilidades Análisis de riesgos

© Autoridad Europea de Valores y Mercados, París, 2025. Reservados todos los derechos. Se pueden reproducir o traducir breves extractos siempre que se cite adecuadamente la fuente. Referencia legal para este informe: Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/77/CE de la Comisión, artículo 32 «Evaluación de la evolución del mercado, incluidas las pruebas de resistencia», «1. La Autoridad supervisará
y evaluar la evolución del mercado en su ámbito de competencia y, cuando sea necesario, informar a la Autoridad Europea de Supervisión (Autoridad Bancaria Europea), a la Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación), a la Junta Europea de Riesgo Sistémico, al Parlamento Europeo, al Consejo y a la Comisión sobre las tendencias microprudenciales pertinentes, los posibles riesgos y las vulnerabilidades. La Autoridad incluirá en sus evaluaciones un análisis de los mercados en los que operan los participantes en los mercados financieros y una evaluación del impacto de la posible evolución del mercado en dichos participantes. La información contenida en esta publicación, incluidos textos, gráficos y datos, tiene exclusivamente fines analíticos. No proporciona previsiones ni asesoramiento de inversión, ni perjudica, excluye ni influye en modo alguno en las obligaciones regulatorias o de supervisión pasadas, presentes o futuras de los participantes en el mercado. Los gráficos y análisis de este informe se basan, total o parcialmente, en datos que no son propiedad de la ESMA, incluidos los de proveedores de datos comerciales y autoridades públicas. La ESMA utiliza estos datos de buena fe y no se responsabiliza de su exactitud o integridad. La ESMA se compromete a mejorar constantemente sus fuentes de datos y se reserva el derecho de modificarlas en cualquier momento. Los datos de terceros utilizados en esta publicación pueden estar sujetos a descargos de responsabilidad específicos del proveedor, especialmente en lo que respecta a su propiedad, su reutilización por parte de terceros y, en particular, a su exactitud, integridad o actualidad, así como a la responsabilidad del proveedor en relación con ello. Para obtener más información sobre estos descargos de responsabilidad, consulte los sitios web de los proveedores de datos, cuyos nombres se indican a lo largo de este informe. Cuando se utilizan datos de terceros para crear un gráfico o una tabla, o para realizar un análisis, se identifica al tercero y se le atribuye la fuente. En todos los casos, se cita a la ESMA por defecto como fuente, lo que refleja cualquier gestión de datos o depuración, procesamiento, comparación, análisis, edición u otros ajustes realizados a los datos brutos.

Autoridad Europea de Valores y Mercados (ESMA)
Departamento de Economía, Estabilidad Financiera y Riesgos
201-203 Calle de Bercy
FR-75012 París

análisis.de.riesgos@esma.europa.eu

ESMA - 201-203 rue de Bercy - CS 80910 - 75589 Paris Cedex 12 - Francia - www.esma.europa.eu
Foto de portada: Imagen Microsoft 365

Machine Translated by Google

Estabilidad financiera

Riesgos operativos y cibernéticos en Mercados financieros de la UE: medición y simulación de tensiones

Contacto: onofrio.panzarino@esma.europa.eu1 y steffen.kern@esma.europa.eu

Resumen

El riesgo cibernético se ha convertido en una amenaza creciente para la estabilidad financiera. La frecuencia y la sofisticación de los incidentes han aumentado en los últimos años, y su impacto financiero es significativo y creciente.

La medición y el seguimiento de las ciberamenazas desde la perspectiva de la estabilidad financiera plantean desafíos considerables. El panorama de amenazas, dinámico y en rápida evolución, sumado a la limitada visibilidad de los incidentes, dificulta una evaluación y valoración precisa de los riesgos. En Europa, la Ley de Resiliencia Operativa Digital (DORA) tendrá un impacto concreto en la visibilidad de los incidentes. Introdujo un marco armonizado e integral para la resiliencia operativa digital de las instituciones financieras de la UE y estableció un sistema de notificación de incidentes graves relacionados con las tecnologías de la información y la comunicación (TIC) por parte de dichas instituciones.

Este artículo profundiza en la importancia sistémica del ciberriesgo. Explora marcos conceptuales para examinar cómo los incidentes individuales pueden volverse sistémicos, centrándose en la exposición a las ciberamenazas, la propagación del impacto a través del sistema y su impacto.

El documento también presenta los resultados de un análisis de simulación realizado en el mercado de repos de la UE, Se examinan escenarios en los que un ciberincidente hipotético interrumpe las operaciones de liquidación de los principales participantes del mercado. Los resultados indican que las interrupciones operativas en algunas instituciones críticas pueden provocar una escasez de liquidez temporal pero grave, tanto a nivel del sistema como de la contraparte, con efectos de red generalizados.

El artículo subraya la necesidad de contar con marcos sólidos de información sobre incidentes cibernéticos, el desarrollo de métricas de riesgo y herramientas de monitoreo basadas en nuevas fuentes de datos de información, y el uso de modelos conceptuales y simulaciones para mejorar la evaluación de los riesgos cibernéticos desde una perspectiva de estabilidad financiera.

Las mejoras que aquí se presentan complementarán el marco de seguimiento del riesgo operativo de la ESMA.2

1 Este artículo fue escrito por Onofrio PANZARINO, asesor de la Dirección de Supervisión de Mercados y Sistemas de Pago del Banco de Italia, durante una comisión de servicio en la ESMA de mayo de 2024 a abril de 2025. La ESMA agradece al Sr. Panzarino sus invaluables contribuciones al trabajo analítico y de monitoreo de riesgos de la ESR.

2 ESMA, “Evaluación del riesgo operativo: el enfoque de la ESMA”, Informe de la ESMA sobre tendencias, riesgos y vulnerabilidades n.º 1, 2018, págs. 68 y siguientes.

Machine Translated by Google

Introducción

El riesgo cibernético está surgiendo como una preocupación creciente para estabilidad financiera. En los últimos años se ha observado un aumento constante en el número, la escala y la complejidad de los incidentes. 3 El software y las herramientas maliciosos se han vuelto más sofisticados y
Cada vez están más disponibles, lo que les permite atacar sistemas vulnerables con mayor facilidad y eficacia. Las instituciones financieras siguen siendo uno de los principales objetivos de los ciberataques.

El riesgo cibernético se diferencia de otros tipos de riesgo operativo en muchos aspectos y plantea desafíos únicos.
Surge de vulnerabilidades tecnológicas y
interrupciones operativas pero pueden tener consecuencias de gran alcance
Efectos que trascienden los sistemas informáticos y abarcan categorías de riesgo más tradicionales, como crisis de liquidez, efectos de contagio o disrupciones generalizadas del mercado. El ciberriesgo también es complejo de monitorizar y evaluar. Su naturaleza dinámica y en rápida evolución, junto con la escasez de datos históricos, dificulta su seguimiento y cuantificación precisos.

Este artículo examina estos aspectos con más detalle y profundiza en la importancia del riesgo cibernético desde una perspectiva de estabilidad financiera.
El artículo está estructurado de la siguiente manera:

- En primer lugar, exploramos la creciente frecuencia y escala de los incidentes cibernéticos, los factores que impulsan estas tendencias. También explicamos los desafíos.
  para mejorar el seguimiento y la medición de riesgos
  y cómo se informa sobre incidentes cibernéticos según DORA ayudará a mitigar estos desafíos.
- La segunda parte del artículo examina los marcos conceptuales, los enfoques de modelado y el análisis de simulación para

  Se evalúa el riesgo cibernético y su impacto en la estabilidad financiera. Además, se presenta un ejercicio de simulación de estrés realizado en el mercado de repos de la UE.

Las mejoras presentadas en este artículo complementarán el marco de seguimiento del riesgo operativo de la ESMA4 y el trabajo anterior sobre resiliencia operativa.5

El riesgo cibernético como una amenaza creciente para la estabilidad financiera

El riesgo cibernético puede definirse como la combinación de la probabilidad de ocurrencia de incidentes cibernéticos y su impacto en el sistema financiero. Los incidentes cibernéticos son eventos, maliciosos o no, que comprometen la ciberseguridad de los sistemas informáticos o infringen los procedimientos y normas operativas. 6

Los riesgos cibernéticos tienen características únicas que los distinguen de los riesgos financieros tradicionales, como el riesgo de mercado, de crédito y de liquidez.

- Fuente de amenaza: Los riesgos cibernéticos provienen de amenazas digitales dirigidas a los sistemas de TI, la infraestructura y la seguridad de los datos, a menudo debido a Vulnerabilidades tecnológicas o actores maliciosos. Los riesgos financieros tienen causas económicas.
  como fluctuaciones del mercado, financieras
  recesiones, problemas de liquidez o impagos.
- Alcance del impacto: Las implicaciones de los cibershocks pueden ser generalizadas y extenderse más allá
  Los sistemas de TI afectan la integridad de los datos, las operaciones comerciales, la reputación y la confianza del consumidor. Por el contrario, los riesgos financieros influyen principalmente en la rentabilidad, el rendimiento de las inversiones y las condiciones económicas.
- Monitoreo y medición de riesgos: En términos de monitoreo de riesgos, las ciberamenazas requieren vigilancia en tiempo real, auditorías de seguridad continuas y mecanismos de respuesta rápida, mientras que los riesgos financieros suelen evaluarse mediante evaluaciones periódicas basadas en datos históricos y modelos financieros consolidados. En términos más generales, la gestión de riesgos cibernéticos es dinámica y adaptable,
  respondiendo a las amenazas en constante evolución, mientras que la evaluación de riesgos financieros suele basarse en marcos más estructurados y predictivos.

  Basado en la teoría económica y financiera.

Cuantificar el riesgo cibernético sigue siendo especialmente difícil debido al panorama de amenazas en constante evolución, el limitado historial y las complejas interdependencias dentro de los sistemas financieros. Las siguientes secciones analizarán estos aspectos con mayor detalle.

3 Véase, por ejemplo, ESRB (2024), ENISA (2024), ECB (2025).

4 ESMA, “Evaluación del riesgo operativo: el enfoque de la ESMA”, Informe de la ESMA sobre tendencias, riesgos y vulnerabilidades n.º 1, 2018, págs. 68 y siguientes.

5 ESMA, “Un marco para evaluar la resiliencia operativa”, Informe de la ESMA sobre tendencias, riesgos y vulnerabilidades, Análisis de riesgos TRV, 19 de diciembre de 2022.

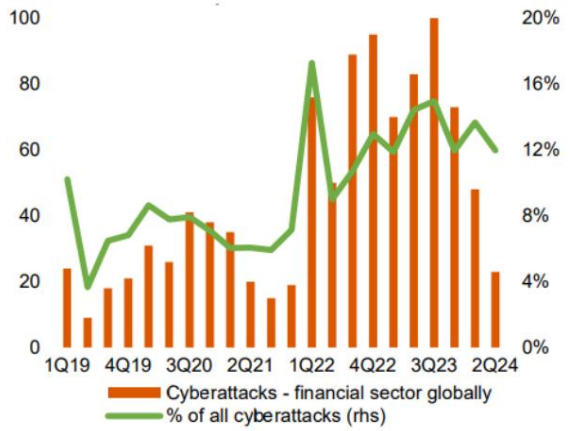
6 Esta definición de riesgo cibernético está tomada del Léxico Cibernético desarrollado por el FSB (2018).

Machine Translated by Google

Relevancia, crecimiento y factores impulsores

La frecuencia y sofisticación de los ciberataques
Han aumentado en los últimos años. A pesar de que la información fragmentada y las divulgaciones voluntarias limitan la disponibilidad de datos exhaustivos, la evidencia existente indica sistemáticamente una tendencia al alza en los incidentes cibernéticos, con un aumento adicional tras la pandemia mundial de COVID-19.
Según el FMI (2024), el número de incidentes cibernéticos denunciados casi se ha duplicado desde el inicio de la pandemia. Datos de otras fuentes.
muestra las mismas tendencias. El Centro de Recursos contra el Robo de Identidad (2020) reporta 12,250 filtraciones de datos en un período de 16 años, de las cuales aproximadamente la mitad ocurrieron en los últimos cinco años de este período. Los datos de la Universidad de Maryland (Base de Datos de Eventos Cibernéticos CISSM) subrayan que el número de ciberataques ha sido históricamente alto en los últimos cinco años (ver Gráfico 1).

Gráfico 1
Ciberataques a entidades del sector financiero
Mayor relevancia de los eventos cibernéticos



Nota: Ciberataques a entidades del sector financiero a nivel mundial por trimestre, incidentes reconocidos públicamente. Para más detalles, véase Harry, C. y Gallagher, N. (2018). Clasificación de cibereventos.
Revista de Guerra de Información, 17(3), 17-31.
Fuente: Base de datos de ataques cibernéticos CISSM de la Universidad de Maryland, ESMA.

Las ciberamenazas siguen siendo los principales riesgos identificados por expertos del sector y autoridades reguladoras de todo el mundo, y se prevé que la frecuencia de incidentes siga aumentando. Las agencias de calificación crediticia han comenzado a incorporar el riesgo cibernético en sus evaluaciones crediticias. Un informe reciente de la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2024) También destaca un aumento sustancial en la Variedad de ciberataques. Esta variedad abarca no solo el ransomware, que puede paralizar las operaciones, como se ejemplifica más adelante en el caso práctico de ICBC, sino también otras amenazas potentes, como los ataques de denegación de servicio distribuido (DDoS) a gran escala, dirigidos a interrumpir la disponibilidad del servicio; las sofisticadas filtraciones de datos dirigidas al robo de información confidencial de clientes o de propiedad exclusiva; y los ataques cada vez más frecuentes a la cadena de suministro de software, que pueden introducir vulnerabilidades en numerosas entidades interconectadas. Cada uno de estos vectores de ataque puede tener distintos impactos financieros y operativos iniciales y seguir distintos mecanismos de propagación dentro del ecosistema financiero, lo que podría requerir medidas preventivas, técnicas de detección y estrategias de respuesta específicas, más allá de la planificación general para la interrupción operativa.

Las consecuencias financieras de los incidentes cibernéticos son significativas y están en aumento. Desde 2020, las pérdidas relacionadas con la ciberseguridad han ascendido a casi 28 000 millones de dólares, según el FMI (2024). Sin embargo, el panorama más amplio...
Los costos del ciberdelito podrían ser mucho mayores si también se consideran las pérdidas indirectas asociadas al evento, como la pérdida de confianza y el daño a la reputación. 7 Por ejemplo, algunos estudios (p. ej., Jamilov, Rey y Tahoun, 2023) estiman que el costo global del ciberdelito alcanza los 200 000 millones de dólares anuales. Sin embargo, las cifras varían considerablemente, lo que refleja las dificultades para una cuantificación precisa, las diferentes metodologías y el alcance de las pérdidas directas e indirectas incluidas.
Según otros estudios, el impacto estimado puede oscilar entre el 1 y el 10 por ciento del PIB mundial, y las previsiones de la industria sugieren que estos costos seguirán aumentando en el futuro (véase, por ejemplo, Centro de Estudios Estratégicos e Internacionales, 2020; ENISA, 2016; Statista, 2022; Embroker, 2024).

Varios factores contribuyen al aumento de la frecuencia y gravedad de los ataques cibernéticos:

- Expansión de la conectividad digital: El rápido crecimiento de la infraestructura digital ha ampliado la exposición a los riesgos cibernéticos (véase la sección «Exposición ex ante a las ciberamenazas» para un análisis de este aspecto). La pandemia de COVID-19 ha acentuado aún más la dependencia de la tecnología y la innovación financiera, exponiendo vulnerabilidades, especialmente con el auge del teletrabajo.

- Avances en las técnicas cibercriminales: Los actores maliciosos continúan desarrollando e implementando herramientas más sofisticadas, que son

7 Las pérdidas directas incluyen, por ejemplo, la pérdida de ingresos comerciales debido a interrupciones operativas, el monto de la extorsión o la cantidad gastada para remediar el daño.
Las pérdidas indirectas incluyen daño a la reputación y pérdida de oportunidades futuras. negocios y reducción de la productividad. Consulte las siguientes secciones para obtener más detalles sobre la distinción entre pérdidas directas e indirectas.

Machine Translated by Google

También cada vez más disponible para su compra por otros individuos o grupos, generalmente con fines de lucro (un modelo conocido como 'ciberdelincuencia') como servicio'), lo que permite que una gama más amplia de perpetradores lleven a cabo ataques.

– Contexto geopolítico: La geopolítica siguió siendo reconocida como un fuerte impulsor de operaciones cibernéticas maliciosas (ENISA, 2024). Los riesgos geopolíticos están aumentando y son globales. Los conflictos y las tensiones, incluida la invasión de Ucrania por parte de Rusia y los disturbios en Oriente Medio, han provocado picos de ciberataques. 8

Las instituciones financieras se encuentran entre las entidades más atacadas,9 ya que suelen manejar grandes volúmenes de datos de consumidores y activos importantes, lo que las hace atractivas para los ciberdelincuentes.
Los ciberataques a estas entidades podrían causar perturbaciones importantes en la sociedad y la actividad económica.

Estudio de caso: El ataque de ransomware en ICBC Financial Services

El 8 de noviembre de 2023, un grupo de ransomware,10 Se cree que una organización cibercriminal altamente sofisticada logró infiltrarse en los sistemas informáticos de ICBC Financial Services (ICBC FS), una filial estadounidense de servicios financieros del Banco Industrial y Comercial de China (ICBC). La filial es propiedad exclusiva de ICBC y se dedica principalmente a prestar servicios de custodia a clientes institucionales, incluyendo servicios globales de compensación, ejecución y financiación.

El ataque causó una interrupción significativa en las operaciones del banco e interrumpió sus sistemas operativos, incluidos aquellos utilizados para compensar transacciones de bonos del Tesoro de Estados Unidos y transacciones de financiamiento de repos. Esto provocó un retraso temporal en el pago a sus contrapartes. Según diversos informes de prensa, la interrupción provocó que ICBC FS adeudara temporalmente a BNY Mellon aproximadamente 9000 millones de dólares, una cantidad muy superior a su capital neto.¹¹

Aunque no se conoce con exactitud el alcance del acontecimiento, Claro, un análisis de Fitch Ratings (2023) ofreció explicaciones de por qué la perturbación del mercado del Tesoro causada por el ataque fue, en general, limitada y no afectó su funcionamiento (Reuters, 2023a). En primer lugar, ICBC FS resolvió rápidamente pagos pendientes poco después de la Ciberataque, gracias a una inyección de liquidez de emergencia de su banco matriz. En segundo lugar, el tamaño de ICBC FS es relativamente pequeño en comparación con su banco matriz (0,4 % de los activos totales de ICBC al final del primer semestre de 2023), cuyo negocio principal se centra en su mercado principal, China. Además, la arquitectura de red segmentada del banco — con los sistemas de ICBC FS operando independientemente de los del grupo matriz— también ayudó a evitar que la disrupción se extendiera más.

A pesar de la perturbación contenida en este caso, persisten las preocupaciones de que un ataque similar a una institución financiera que carece de un apoyo adecuado de los accionistas y de liquidez de emergencia podría desencadenar eventos de incumplimiento, con implicaciones potencialmente significativas para la estabilidad financiera.

Desafíos e iniciativas en la notificación de incidentes cibernéticos

A pesar de la creciente relevancia de las ciberamenazas como posibles fuentes de disrupción sistémica, la falta general de información sobre ellas sigue siendo un obstáculo clave tanto para los participantes del mercado como para las autoridades a la hora de realizar evaluaciones y análisis de riesgos exhaustivos.

La información pública disponible sobre cibereventos suele ser escasa o de mala calidad. Esto se debe en gran medida a problemas de reputación, ya que las empresas se enfrentan a... Desincentivos para divulgar voluntariamente fallos operativos que podrían socavar la confianza y perjudicar su negocio. Además, la falta de requisitos formales para reportar incidentes cibernéticos en muchas jurisdicciones agrava el problema. La información disponible sobre eventos cibernéticos también está dispersa en múltiples fuentes, lo que dificulta aún más obtener una visión completa del panorama de ciberamenazas. Esto se ve agravado por el retraso en la presentación de informes, que distorsiona aún más la percepción de la frecuencia y la gravedad de los incidentes en los períodos más recientes.

La falta de datos e información fiables puede llevar a subestimar el riesgo y el verdadero impacto de los ciberataques. En última instancia, esto también reduce la capacidad de tomar las medidas adecuadas para prevenir o mitigar las ciberamenazas.

8 Véase, por ejemplo, FMI (2024).

9 Según algunas estimaciones de la industria (BCG, 2019), las empresas financieras tienen 300 veces más probabilidades que otras empresas de ser objeto de un ciberataque.

10 La violación fue reivindicada por un grupo cibercriminal llamado Lockbit, que en el pasado ha pirateado algunas de las... Las organizaciones más grandes roban y filtran sus datos confidenciales si no pagan un rescate. Según funcionarios estadounidenses, se ha convertido en la mayor amenaza de ransomware del mundo (Reuters, 2024).

11 Véase, por ejemplo, Reuters (2023b), The Banker (2023).

Machine Translated by Google

Mejorar el seguimiento y la monitorización de riesgos y comprensión de las amenazas cibernéticas

La información sobre incidentes cibernéticos es crucial para tomar medidas eficaces y promover la estabilidad financiera (FSB, 2021). La falta de datos completos es
De hecho, constituye un impedimento crítico para una supervisión eficaz, las evaluaciones de estabilidad financiera y
Gestión de riesgos a nivel de empresa.

Se están realizando esfuerzos a nivel mundial para mejorar la resiliencia operativa ante las amenazas cibernéticas.
Los organismos de normalización, los reguladores financieros y los grupos industriales están combinando sus esfuerzos para construir sistemas más resilientes, por ejemplo, desarrollando directrices políticas para fortalecer la resiliencia cibernética, considerando los riesgos cibernéticos en evaluaciones de estabilidad interna o financiera, o en ejercicios de supervisión o de estrés interno. 12 Estas iniciativas abordan diferentes aspectos del riesgo cibernético y contribuyen a su mitigación.

Dado que las ciberamenazas son inherentemente transfronterizas y que muchas grandes instituciones financieras y proveedores externos críticos operan a escala global, la cooperación y coordinación internacionales eficaces entre las autoridades reguladoras y supervisoras son fundamentales. Esto incluye esforzarse por lograr una mayor armonización de las expectativas regulatorias cuando sea apropiado para evitar la fragmentación y facilitar el cumplimiento normativo de las empresas globales, establecer protocolos claros para el intercambio transfronterizo de información durante incidentes graves y fomentar plataformas internacionales para el intercambio de buenas prácticas en ciberresiliencia e inteligencia de amenazas para contrarrestar con mayor eficacia a los ciberadversarios globales sofisticados.

Las iniciativas clave también incluyen el establecimiento de marcos sólidos de información que exigen a las organizaciones proporcionar informes oportunos y detallados sobre incidentes cibernéticos a las autoridades competentes. Estas medidas buscan subsanar las lagunas de información y fomentar la acción colectiva para abordar los riesgos digitales.

En Europa, la Ley de Resiliencia Operativa Digital (DORA) tendrá un impacto concreto en este ámbito. Introduce un marco armonizado e integral para la resiliencia operativa digital de las instituciones financieras de la UE. También estableció un régimen de notificación de incidentes graves relacionados con las tecnologías de la información y la comunicación (TIC).

Instituciones financieras de la UE. El marco abarca aspectos relevantes de los cibereventos, entre ellos:

- La institución afectada (incluida la clasificación sectorial);
- La naturaleza del incidente (por ejemplo, relacionado con la ciberseguridad, una falla del sistema o un evento externo);
- La fecha y hora del restablecimiento de los servicios;
- El número de clientes, contrapartes y transacciones afectadas por el incidente;
- Los costos y pérdidas financieras incurridos;
- Si el incidente se originó por un proveedor de servicios externo que respalda operaciones comerciales críticas.

El régimen de presentación de informes entró en vigor el 17 de enero de 2025.

Al establecer un marco de informes estandarizado y obligatorio, la iniciativa tiene el potencial de mejorar significativamente la capacidad de identificar, rastrear y comprender los riesgos cibernéticos. También puede permitir a las autoridades identificar vulnerabilidades sistémicas, desarrollar herramientas de monitoreo más precisas y crear indicadores de riesgo para rastrear tendencias en...
Incidentes cibernéticos en distintos sectores y regiones a lo largo del tiempo. Además, puede proporcionar información valiosa sobre los canales de contagio y las vulnerabilidades sistémicas mediante el análisis de las complejas redes de interdependencias de las TIC entre proveedores de servicios externos y entidades financieras.
Esto permite una mejor evaluación de la resiliencia y la capacidad de respuesta del sistema financiero a las amenazas cibernéticas, así como de cómo estas amenazas evolucionan con el tiempo.

Además de la notificación de incidentes, DORA abarca otras iniciativas destinadas a mejorar la capacidad del sector financiero de la UE para prevenir, responder y recuperarse de las interrupciones de las TIC. Estas iniciativas también pueden facilitar una modelización y cuantificación más precisas del riesgo cibernético. Algunos ejemplos incluyen la notificación de ciberamenazas significativas, la realización de pruebas de penetración basadas en amenazas y el establecimiento de registros de proveedores externos de servicios de TIC.

Si bien DORA proporciona un marco integral para la resiliencia operativa digital que se extiende más allá de los informes, las medidas de defensa proactivas y en constante evolución de las empresas siguen siendo

[12] Por nombrar solo algunos, el FSB (2018) desarrolló un Léxico Cibernético para estandarizar la comunicación sobre riesgos cibernéticos. En la UE, se ha reforzado el mandato de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), y las Autoridades Europeas de Supervisión (AES) han publicado directrices sobre la gestión de riesgos de las TIC. Diversos marcos, como la Directiva NIS y TIBER-EU, abordan los riesgos cibernéticos. El BCE ha creado el Consejo de Ciberresiliencia del Euro y ha realizado pruebas de resistencia a los bancos (BCE, 2024); el G7 ha realizado ejercicios cibernéticos interjurisdiccionales.

Machine Translated by Google

Es crucial. Esto incluye la inversión sostenida en tecnologías de seguridad avanzadas, como sistemas de detección de amenazas basados en IA y detección de anomalías; la realización de pruebas periódicas y rigurosas para identificar y remediar vulnerabilidades de forma proactiva; el desarrollo, la prueba y la actualización periódica de sólidos planes de continuidad de negocio (PCN) y planes de respuesta a incidentes (PRI); y la capacitación integral y continua en ciberseguridad para todo el personal. Además, el fomento de plataformas para el intercambio voluntario y oportuno de inteligencia sobre amenazas entre instituciones financieras puede complementar los mecanismos formales de denuncia y mejorar la preparación y la situación colectivas.

conciencia

Modelos para analizar eventos cibernéticos sistémicos

Las ciberamenazas se han convertido cada vez más en un riesgo significativo para la estabilidad financiera, como se destacó en secciones anteriores. Economistas, participantes del mercado y autoridades financieras siguen destacando la urgente necesidad de profundizar
Comprender las amenazas cibernéticas y desarrollar capacidad de evaluar su impacto desde una perspectiva sistémica (Duffie y Younger, 2019; Kashyap y Wetherilt, 2019).

A lo largo de los años, se han desarrollado varios modelos conceptuales para explorar cómo eventos individuales pueden escalar hasta convertirse en una amenaza sistémica y para navegar mejor la compleja red de mecanismos y vínculos que entran en juego en los ecosistemas financieros modernos. Ejemplos notables que se basan en investigaciones previas[13] incluyen la JERS (2020), el BCE (2025) y el FMI (2024).

Según muchos estudios, el desarrollo de un cibershock se puede descomponer en general en
tres etapas:

(1) la exposición a amenazas cibernéticas;

(2) la liberación del shock y su propagación a través del sistema financiero; y

(3) las consecuencias macroeconómicas y financieras resultantes, que afectan a funciones económicas clave.

Cada etapa se analiza en detalle en las siguientes secciones.

Exposición ex ante a amenazas cibernéticas

El primer aspecto a considerar al estudiar un evento cibernético es la vulnerabilidad de la empresa a este riesgo, es decir, su exposición ex ante. En principio, cada empresa tiene diferentes niveles de exposición a los riesgos cibernéticos, dependiendo de diversos factores. Estos pueden ser específicos de la empresa o externos.

Los factores específicos de cada empresa se relacionan con el individuo Características de cada empresa. Por ejemplo, las empresas con mayor presencia digital, por ejemplo, si su actividad principal depende en gran medida de las nuevas tecnologías o requiere una alta conectividad tecnológica, pueden ser más vulnerables a las ciberamenazas. Por el contrario, medidas proactivas, como invertir en ciberseguridad, capacitar a los empleados y concienciar sobre la ciberseguridad, pueden reducir la exposición a los ciberataques y mitigar los riesgos.[14]

Los factores externos incluyen el contexto geopolítico y el entorno regulatorio. Empresas
Las empresas que operan en regiones con tensiones geopolíticas pueden estar más expuestas a ciberataques (FMI, 2024). De igual manera, las jurisdicciones con leyes cibernéticas menos desarrolladas pueden generar mayor vulnerabilidad para las empresas.

Ambos niveles de exposición evolucionan con el tiempo, influenciados por los cambios en el desarrollo y la adopción de tecnologías. Si bien estos avances pueden ser beneficiosos para la innovación y los servicios al consumidor, también pueden aumentar inadvertidamente la exposición a las ciberamenazas.

Liberación y transmisión del amortiguador

La segunda fase se centra en la aparición de cibershocks y su amplificación en todo el sistema financiero. Los cibereventos, según la definición del FSB (2018), se refieren a sucesos, maliciosos o no, que se desencadenan dentro de los sistemas o redes de TI.
Una vez desencadenado, un evento cibernético puede derivar en riesgos más tradicionales, como crisis de liquidez y contagio financiero, y amenazar la estabilidad financiera a través de varios canales.

En primer lugar, la falta temporal de disponibilidad de servicios financieros prestados por entidades críticas del sistema financiero puede conducir a una disfunción del mercado, dada la posible falta de sustitutos disponibles.

En segundo lugar, una pérdida de confianza puede erosionar la confianza en las instituciones y los mercados financieros, lo que lleva a un comportamiento de "corrida masiva" y a mayores riesgos de liquidez; por ejemplo, mediante retiros de depósitos o corridas bancarias, también denominadas en este contexto como "corridas cibernéticas".

[13] Véase, por ejemplo, Ross (2020), Kaffenberger y Kopp (2019), Healey et al. (2018), y Brando et al. (2022).

[14] Esto significa prácticas de seguridad en línea y salud del sistema, como antimalware y autenticación multifactor.

Machine Translated by Google

(Duffie y Younger, 2019). Una pérdida de confianza puede tener un efecto dominó, desencadenando canales potencialmente contagiosos y liquidaciones forzosas de activos, incluso en instituciones no directamente afectadas (Brando et al., 2022).

En tercer lugar, las interrupciones en una parte del sistema pueden Propagación a otros, lo que genera efectos de contagio y una mayor inestabilidad financiera. En el caso de los cibereventos, los canales a través de los cuales se puede transmitir el shock pueden involucrar no solo vínculos comerciales (por ejemplo, relaciones comerciales, vínculos comerciales), sino también vínculos más complejos y a menudo no reconocidos entre empresas, incluyendo una capa de exposición a tecnologías compartidas y proveedores de servicios externos. Estos proveedores y su interconexión con otras instituciones financieras e infraestructuras de mercado añaden una nueva capa de interdependencias que puede exacerbar las vulnerabilidades. Incorporar este tipo de relaciones es crucial al realizar evaluaciones de riesgos (Bouveret y Herraez, 2022).

Impacto

La tercera etapa evalúa el punto en el que un evento cibernético puede tener un impacto sistémico.
La estabilidad financiera depende de la capacidad del sistema financiero para proporcionar funciones económicas clave (FEC) en caso de un incidente cibernético.
(JERS, 2022). Esta fase considera si un incidente cibernético afecta negativamente los resultados macroeconómicos hasta el punto de que el sistema ya no puede proporcionar un factor de riesgo clave (KEF) y absorber o mitigar el impacto. Ejemplos de deterioro de los KEF incluyen la reducción en la provisión de crédito, la interrupción de servicios financieros críticos como los sistemas de pago o liquidación, la materialización de un shock financiero sistémico como la escasez de liquidez o el deterioro del funcionamiento del mercado.

Las autoridades pueden emplear umbrales de impacto para cuantificar la resiliencia. El umbral superior define el impacto máximo que el sistema financiero puede soportar, mientras que el inferior indica el nivel operativo mínimo de las instituciones y funciones. La diferencia entre estos umbrales refleja la capacidad del sistema para absorber shocks y mantener la estabilidad (JERS, 2023). La identificación de estos umbrales permite a las autoridades evaluar la resiliencia de sus empresas, infraestructuras y mercados financieros, y apoyar el desarrollo de capacidades de respuesta, coordinación e intervención ante crisis. Se está trabajando en el desarrollo de enfoques para identificar estos umbrales.

Para ilustrar mejor cómo un evento cibernético puede convertirse en un riesgo sistémico, el modelo anterior se ha aplicado a un ejercicio de simulación centrado en el Mercado europeo de repos. El análisis se presenta en la siguiente sección.

Medición de riesgos y simulaciones de estrés

Como se destaca, el impacto de los incidentes cibernéticos puede ser de largo alcance, alterando potencialmente funciones críticas del mercado y convirtiéndose en un riesgo para la estabilidad financiera.

Evaluar la relevancia sistémica de las ciberamenazas es fundamental desde la perspectiva de la estabilidad financiera y requiere una indicación de la magnitud y la criticidad de las posibles pérdidas en caso de interrupciones relacionadas con la ciberseguridad. Investigaciones recientes, como la de Bouveret (2019), destacan marcos para cuantificar el ciberriesgo. Estos estudios demuestran cómo los modelos utilizados para la evaluación del riesgo operativo en los bancos pueden adaptarse para analizar el ciberriesgo.

Los resultados indican que las pérdidas estimadas pueden ser sustanciales, especialmente cuando se las compara con el tamaño del mercado de seguros cibernéticos, y la distribución de estas pérdidas puede presentar colas pesadas.

De manera más general, los marcos de modelado y las simulaciones de estrés pueden ser herramientas poderosas para explorar estos aspectos y, en el contexto de las evaluaciones de riesgos, pueden proporcionar información útil sobre:

- Materialidad del choque, al proporcionar una descripción detallada Evaluación de la interrupción operativa y el posible impacto financiero que podría derivar de un ciberincidente. Esta cuantificación es crucial para comprender la magnitud de la amenaza y elaborar estrategias de mitigación adecuadas.

- Canales de amplificación, ya que los incidentes cibernéticos pueden propagarse a través de sistemas y mercados interconectados, amplificando su impacto.
  El análisis de simulación puede ayudar a identificar estos canales y proporcionar una mejor comprensión de cómo un incidente localizado puede convertirse en un riesgo sistémico.

Vulnerabilidades ex ante, mediante la simulación de escenarios que permiten a las instituciones financieras y a las autoridades identificar las debilidades del sistema. Este enfoque proactivo permite fortalecer las defensas y mejorar la resiliencia general del sistema.

Los enfoques de modelado adoptados en este estudio También se alinea con la ESMA más amplia (2018) Estrategia de riesgo operacional, complementando las evaluaciones cualitativas de riesgo operacional con marcos analíticos que permitan mapear los canales de propagación y los vínculos sistémicos. Esto es particularmente importante cuando se manifiesta el riesgo cibernético

Machine Translated by Google

Debido a interrupciones a nivel de infraestructura y a la dependencia de terceros, el análisis basado en simulación ofrece una cuantificación prospectiva de la exposición a eventos cibernéticos y podría servir como prototipo para el desarrollo de futuros indicadores cuantitativos de riesgo operativo.

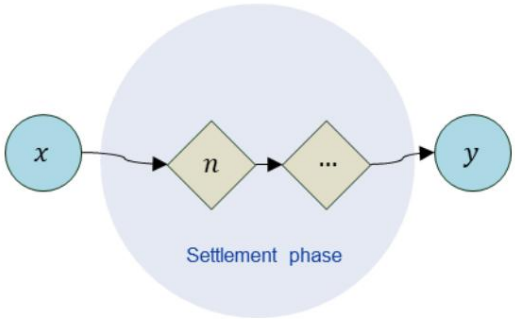
La siguiente sección presenta un ejercicio de simulación diseñado para estudiar el impacto potencial de un ciberataque que afecte al funcionamiento del mercado de repos en Europa. El análisis se centra en el diseño de un ciberataque hipotético que interrumpa la liquidación de operaciones de repos, similar al ciberataque de ICBC FS en el mercado de bonos del Tesoro estadounidense en noviembre de 2023 (véanse las secciones anteriores).

Las siguientes secciones describen el contexto del ejercicio de simulación, el escenario diseñado, el enfoque para la medición del riesgo y los resultados del análisis.

Gráfico 2

Configuración del mercado

Transacción de recompra estilizada



Nota: Ilustración de una operación de repo entre dos contrapartes, donde una entidad (es decir, el prestatario del repo, y) recibe financiación de otro participante del mercado (es decir, el prestamista del repo, x). Los rombos (por ejemplo, el nodo n) representan los nodos de liquidación en la fase posterior a la negociación de la operación. Son Los participantes directos del CSD que gestionan las operaciones de liquidación, que pueden ser la propia contraparte o un proveedor de servicios externo, son los objetivos del ciberataque considerado en el escenario de estrés analizado.
Fuente: ESMA.

Simulación de estrés: evidencia del mercado de repos de la UE

Los mercados de repos son cruciales desde la perspectiva de la estabilidad financiera. Cumplen diversas funciones, desde la provisión de liquidez a una amplia gama de inversores hasta el intercambio de garantías en el sistema financiero, apoyando así el funcionamiento de los mercados y la economía en general.

Este análisis utiliza datos regulatorios de la Reglamento sobre las operaciones de financiación de valores (SFTR), que proporciona información detallada y granular Información sobre operaciones de repo y repo inverso realizadas por participantes del mercado en Europa. En ESMA (2024) se ofrece una visión general completa del mercado de repos de la UE, basada en la información proporcionada por los participantes del mercado en virtud del SFTR.

Configuración del mercado

Nuestro ejercicio de simulación se basa en escenarios en los que un evento cibernético afecta la capacidad de una institución. para liquidar sus operaciones de repo en un día determinado y Investiga cuantitativamente el impacto resultante en la red de repos más amplia.

El entorno de mercado de referencia para el análisis se ilustra en el Gráfico 2. Muestra un ejemplo estilizado de una operación de repo entre dos contrapartes, donde una entidad (es decir, el prestatario del repo) recibe financiación de otro participante del mercado (es decir, el prestamista del repo). Una vez realizada la operación, debe liquidarse mediante la entrega de valores y la realización de pagos en efectivo entre las partes. La liquidación no se completa hasta que

El prestamista del repo y el prestatario han cumplido con sus obligaciones mutuas, es decir, la entrega de valores para el prestatario del repo y el pago en efectivo para el prestamista.

La gestión de las tareas posteriores a la negociación generalmente la gestionan los departamentos de operaciones de las contrapartes comerciales (véase ICMA, 2023). Para la liquidación, envían instrucciones para la entrega y recepción de valores a los Sistemas de Liquidación de Valores (SLV), operados por depositarios centrales de valores (DCV) nacionales o depositarios centrales de valores (DCVI) internacionales. Las operaciones se liquidan generalmente mediante entrega contra pago, es decir, un mecanismo que vincula la transferencia de valores con la transferencia de efectivo, de tal manera que la entrega de valores se produce solo si se produce la transferencia de efectivo correspondiente.

y viceversa. En consecuencia, si una contraparte no entrega los valores ni el efectivo, la operación no se liquida.

Nodos de asentamiento y dependencias de terceros

La participación directa en los CSD está sujeta a restricciones financieras, operativas y legales que pueden resultar onerosas y costosas para los participantes del mercado.
Invertir en múltiples mercados también requeriría una cuenta en diferentes CSD. En lugar de acceder directamente a los CSD, los inversores pueden optar por recurrir a servicios de liquidación proporcionados por un tercero.

Machine Translated by Google

operaciones como bancos custodios,[15] para liquidar sus transacciones. Para los fines de este análisis, las entidades que gestionan los procesos de liquidación en nombre propio y/o en nombre de sus clientes se denominan nodos de liquidación.

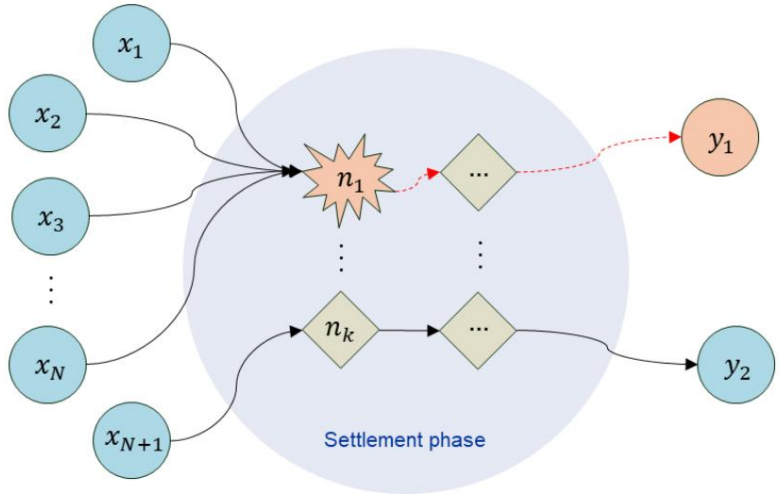
Una característica única del conjunto de datos utilizado en este análisis es que permite la identificación y el mapeo de los nodos de liquidación críticos en la red europea de repos. Las entidades de la UE informan si son miembros directos de un DCV o si, en cambio, dependen de un tercero para liquidar sus operaciones.
transacciones, es decir, los llamados CSD indirectos modelo de participación. En este último caso, las entidades informantes proporcionan detalles para identificar al tercero prestación de los servicios (es decir, código LEI; para referencia, véase ESMA, 2021).

Los nodos de liquidación se muestran como rombos en el Gráfico 2 (p. ej., nodo). Como se mencionó anteriormente, se refieren a los participantes directos del CSD que gestionan las operaciones de liquidación y pueden ser la propia contraparte o un proveedor de servicios externo. Estas entidades son el objetivo del ciberataque considerado en el escenario de estrés analizado.

Gráfico 3

Red de liquidación de repos: un ejemplo estilizado

Cibershock en el escenario analizado



Nota: Ejemplo estilizado de una red de liquidación de repos que muestra nodos de liquidación y dependencias de terceros. En el escenario de estrés analizado, el nodo sufre un incidente cibernético que afecta temporalmente su capacidad para liquidar transacciones. Como resultado del incidente, los repos negociados por las entidades 1 , 2 … no se liquidan según lo previsto y la entidad 1 experimenta una escasez temporal de liquidez; es decir, el efectivo obtenido a través de repos no llega a su balance según lo previsto.

Fuente: ESMA.

Al utilizar información sobre nodos de liquidación críticos en la red de repos, nuestro análisis puede identificar escenarios de estrés en los que una contraparte que recibe financiación de diferentes entidades, pero a través de un nodo de liquidación común, podría verse más afectada por el evento. La interconexión es ampliamente reconocida como un factor clave en las evaluaciones de riesgos para la estabilidad financiera. Como se mencionó en secciones anteriores, los shocks cibernéticos pueden propagarse a través de vínculos que van más allá de las relaciones comerciales, como a través de proveedores de servicios externos. Esto añade un nuevo nivel de... interdependencias que pueden propagar choques y exacerbar las vulnerabilidades.

La financiación proporcionada por prestamistas de repos que no están relacionados entre sí podría verse afectada por el mismo incidente informático si, por ejemplo, ambas entidades dependen del mismo nodo de liquidación. El análisis considera este posible canal de contagio.

Escenario base

Como se destaca, la simulación de estrés se centra en un escenario en el que se produce un incidente cibernético hipotético.

[15] Los custodios ofrecen una amplia gama de servicios, que incluyen liquidación, custodia y todas las operaciones generales posteriores a la negociación relacionadas con el ciclo de vida de los valores financieros. Para más información referencia sobre el modelo de negocio de los bancos custodios y El papel que desempeñan en los ecosistemas financieros modernos (véase Coste et al., 2021).

Machine Translated by Google

Afecta la capacidad operativa de un nodo de liquidación crítico. Por ejemplo, un ciberataque puede afectar temporalmente la disponibilidad de datos relevantes o de los sistemas de comunicación y mensajería de una institución objetivo, como, en este caso, un banco principal que presta servicios de posnegociación a inversores, que podría verse temporalmente imposibilitado de procesar o transmitir pagos a los SLV.

En el escenario diseñado (línea base), el ciberataque se dirige a uno de los 10 nodos de liquidación más grandes de la red europea de repos. Los nodos de liquidación son participantes directos del CSD, como se define en el párrafo anterior. Se asume que, una vez afectado por el ciberataque, el nodo sería...

no puede liquidar todas las operaciones de repo con sus contrapartes, ya sea por cuenta propia o por cuenta de sus clientes (en el caso de intermediarios que prestan servicios de custodia, como los bancos custodios).

Aunque el escenario diseñado se centra en un ciberataque dirigido, es importante destacar que la simulación de estrés y sus resultados seguirían siendo válidos si la interrupción se debiera a un incidente operativo general. Estos podrían incluir, por ejemplo, fallos del sistema informático, errores humanos,

u otros eventos imprevistos que interrumpan de manera similar la capacidad de la entidad para liquidar transacciones.
Por lo tanto, las principales conclusiones del análisis pueden interpretarse como que cubren una gama más amplia de posibles riesgos e impactos de disrupción operativa, en lugar de específicamente los ciberataques.

El gráfico 3 ofrece un ejemplo estilizado de la Escenario base descrito anteriormente. El nodo sufre un incidente cibernético que afecta temporalmente su capacidad para liquidar transacciones. Como resultado del incidente, los repos negociados por las entidades 1 , 2 … no se liquidan según lo previsto y la entidad experimenta una escasez [1] temporal de liquidez; es decir, el efectivo obtenido a través de los repos que se liquidarán ese día no llega a su balance según lo previsto.

Por el contrario, los valores proporcionados como garantía en los repos tampoco se intercambian entre las partes y permanecen (libres de cargas) en el balance del proveedor de la garantía (1 (en el ejemplo). Si bien este artículo se centra en el canal de liquidez, el lado de las garantías también puede explorarse como una posible fuente de riesgo sistémico, ya que los grandes fallos de liquidación podrían socavar la liquidez y el buen funcionamiento de los mercados de valores (véase, por ejemplo, Iyer y Macchiavelli, 2017). Este aspecto se deja para futuras investigaciones.

Una salvedad a este análisis es que la duración del incidente puede ser limitada y las operaciones de TI pueden reanudarse rápidamente, por ejemplo, si la institución afectada cuenta con planes de contingencia operativos eficaces. Además, se asume la falla independientemente de su probabilidad de ocurrencia.

Si bien esta simulación de estrés se centra en el impacto inmediato de un incidente cibernético, una evaluación más amplia debe considerar factores adicionales.

Estos incluyen la capacidad de las empresas para restaurar sus sistemas de TI, la probabilidad de que ocurra el incidente y la disponibilidad de sustitutos comerciales. Las distintas instituciones pueden tener distintas velocidades y capacidades de recuperación, y las interrupciones prolongadas podrían agravar los impactos iniciales. También es crucial considerar cómo podrían reaccionar otros participantes del mercado, como acumular liquidez, recurrir a activos más seguros, liquidar posiciones con las contrapartes afectadas o incluso realizar ventas forzosas si aumentan las presiones de liquidez. El shock inicial podría propagarse aún más a través de estos comportamientos. Por el contrario, medidas de mitigación como la activación de planes integrales de continuidad de negocio y gestión de crisis, respuestas coordinadas de la industria o la búsqueda de sustitutos comerciales podrían cambiar la trayectoria del evento después del impacto inicial.

Si bien estos factores son importantes para las evaluaciones de riesgos, a menudo son difíciles de observar y pueden requerir más modelos e hipótesis.
Además, la información subyacente puede ser escasa o inexacta, lo que dificulta proporcionar estimaciones confiables (véanse las secciones anteriores para un análisis más detallado de las lagunas de datos en el modelado de riesgos cibernéticos).

En cualquier caso, en el escenario analizado, la Una falla operativa tendría un impacto inmediato y directo en la capacidad de las instituciones para llevar a cabo sus negocios diarios y, por un período de tiempo, la incapacidad de procesar o transmitir pagos.
provocaría una escasez temporal de liquidez para contrapartes. En la siguiente sección nos centraremos en cuantificar este impacto potencial.

Enfoque empírico

El objetivo de la simulación de estrés es analizar escenarios en los que un incidente cibernético impide a uno de los mayores participantes del mercado de repos liquidar sus operaciones y cuantificar el potencial impacto del shock en la liquidez de la red de repos.

Como se destacó en secciones anteriores, los incidentes cibernéticos pueden transformarse en riesgos financieros más tradicionales y convertirse en un evento sistémico.
que afectan la prestación de funciones económicas clave, como la concesión de crédito o la prestación de servicios críticos por parte de una infraestructura del mercado financiero. Este análisis se centra en un factor de liquidez clave (FEC) en particular: la provisión de financiación mediante repos y el impacto de un ciberincidente que interrumpe la liquidación de repos para un subconjunto de instituciones críticas, lo que resulta en una falta temporal de liquidez para varias contrapartes.

Machine Translated by Google

Para evaluar la magnitud del posible impacto en la liquidez del ciberataque, seguimos los siguientes pasos. Primero, identificamos el conjunto de los 10 nodos de liquidación más grandes de nuestra muestra (en términos de importes brutos totales de liquidación). Para este análisis, los nodos de liquidación se definen como participantes directos del CSD. Son los objetivos del ciberataque en el escenario (denominados «nodos afectados»). Segundo, para todas las contrapartes conectadas a cada nodo afectado, su posición neta de préstamo de repos se calcula mediante la siguiente fórmula:

– , , . , ,

donde) es el importe pendiente (en miles de millones de EUR) de repos (repos inversos) que se liquidarán al comienzo del día por la contraparte y a través del nodo de liquidación .

En tercer lugar, para cuantificar el impacto del shock, se tomaron en cuenta los siguientes indicadores de riesgo:

— Escasez de liquidez, calculada como la suma del total de préstamos netos repo afectados por el shock, a nivel del sistema y de la contraparte (y expresada en miles de millones de euros).

— Escasez relativa de liquidez, calculada como la proporción del financiamiento repo afectado por el shock, a nivel del sistema y de la contraparte (y expresada en porcentajes).

— Número de entidades afectadas (o "perjudicadas"), es decir, contrapartes para las cuales una parte (o una porción significativa) de su endeudamiento total en el mercado de repos se ve afectado por el shock cibernético (y por lo tanto no se liquida cuando esperado).

Para captar un mayor número de resultados potenciales y aumentar la robustez de los resultados, la simulación se repitió durante 100 días de negociación seleccionados aleatoriamente, y para cada uno de ellos, se repitió en los 10 principales nodos de liquidación (lo que generó 1000 escenarios). Los resultados del análisis se presentan en la siguiente sección.

Tabla 1

Resultados de simulación, estadísticas descriptivas

Material de impacto y generalizado entre las contrapartes de repos

	Media	DE	p5	p10	p25	p50	p75	pág. 90	pág. 95
Nivel del sistema									
Déficit de liquidez, miles de millones de euros	35.2	32.8	0.4	1.1	7.7	25.5	64.8	87.5	96.3
Porcentaje de préstamos afectados, %	6,2	5.7	0.1	0.2	1.4	4.6	11.8	15.1	16.6
Número de contrapartes afectadas	64,1	58.6	6.0	7.0	12.0	61.0	88.0	127,1	198,0
Número de contrapartes deterioradas	31.3	38.5	1.0	2.0	4.0	20.0	43.0	78.0	124.0
Nivel de contraparte									
Déficit de liquidez, millones de euros	735,3	1.923	0,5	1.2	8.0	130,1	541,2	1.767	3.347
Porcentaje de préstamos afectados, %	47,6	39,7	0.1	1.0	8.6	38.9	100.0	100.0	100.0

Nota: Estadísticas descriptivas sobre la distribución de los déficits de liquidez y el número de entidades afectadas, como resultado de un ciberataque dirigido a uno de los 10 principales participantes (nodos) de la RSN. Los indicadores de impacto se calculan a nivel de sistema y de contraparte. La simulación se realiza durante 100 días seleccionados aleatoriamente, de enero de 2023 a junio de 2024.
Fuente: SFTR, cálculo ESMA.

Resultados

Los resultados se muestran en la Tabla 1 y el Gráfico 4.

Según el análisis de simulación de estrés, la interrupción de las operaciones de liquidación en cualquiera de los 10 participantes más importantes en la red de liquidación de repos de la UE se habría asociado con una escasez sustancial de liquidez, de unos 35.000 millones de euros, en promedio, a nivel del sistema.

El impacto no es despreciable si lo comparamos, por ejemplo, con la financiación total en el mercado de repos. Los resultados muestran que, en un día promedio en nuestra

Por ejemplo, alrededor del 6% del total de préstamos repo es potencialmente afectados por el incidente. El impacto financiero del ciberataque puede ser particularmente grave en la mayoría de los escenarios adversos. Como se muestra en el Gráfico 4, la distribución del impacto tiene una cola derecha larga, y la magnitud del impacto puede ser casi...

El triple, llegando a superar el 16% del endeudamiento total en los casos más extremos (percentil 95). Este hallazgo también es consistente con estudios previos que muestran que las pérdidas debidas al riesgo cibernético pueden estar muy sesgadas (Bouveret, 2019).

Machine Translated by Google

El posible shock de liquidez también suele ser generalizado entre las entidades, pudiendo afectar a varias contrapartes. En promedio, más de 60 prestatarios de repos están involucrados en el incidente, cifra que aumenta a más de 100 en la mayoría de los escenarios adversos.

El impacto promedio a nivel de contraparte se estima en alrededor de 750 millones de euros. Esta cifra es elevada y se ve afectada por la presencia de valores atípicos: según los resultados de la simulación, el valor mediano del impacto individual es mucho menor e indica que, en la mitad de los casos, el shock podría...

ser hasta cinco veces más pequeño (es decir, por debajo de 150 millones de euros).

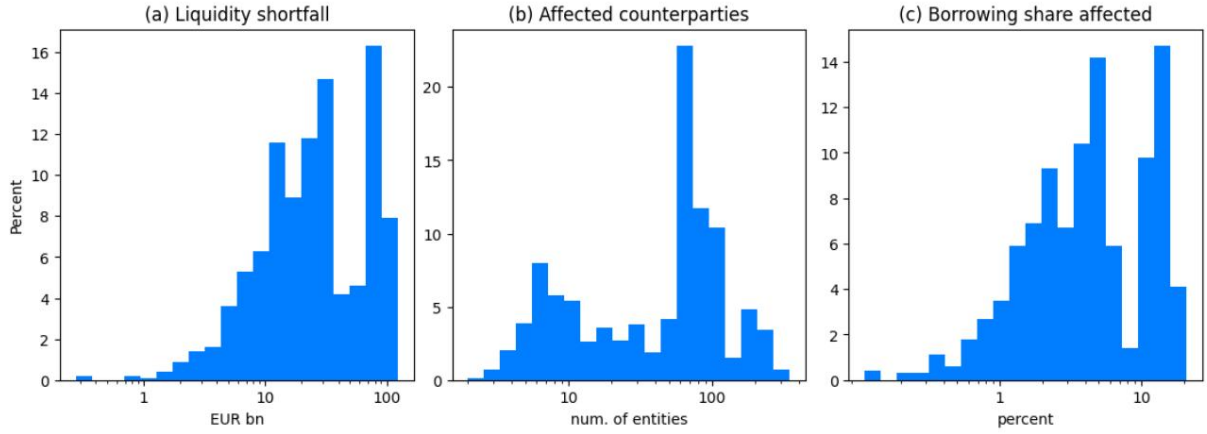
Para analizar con mayor detalle el impacto del cibershock a nivel de empresa, el gráfico 5 muestra la distribución del posible déficit de liquidez que podrían afrontar las contrapartes de repos en los escenarios de estrés analizados. La distribución del impacto se desglosa por sector de la contraparte (gráfico 5, panel b), por participación directa o indirecta en los CSD (es decir, cuando la financiación de repos es proporcionada por prestamistas que dependen o no de terceros que presten servicios de liquidación; gráfico 5, panel c), por la proporción del endeudamiento de la empresa afectado por el evento (a nivel de la empresa; gráfico 5, panel d).

Los resultados de la estimación destacan lo siguiente:
En primer lugar, el incidente informático podría tener un impacto generalizado en todos los sectores, lo que provocaría efectos indirectos en varias contrapartes, siendo las instituciones bancarias principales (como los intermediarios) y las CCP las más afectadas. El déficit temporal de liquidez podría superar los 10 000 millones de euros a nivel individual en ciertos escenarios (véase el gráfico 5, panel b), lo que refleja, por ejemplo, la «centralidad de la red»16.
de algunas entidades de la red de repos de la UE, así como el nivel general de interconexión y

concentración en el mercado (véase, por ejemplo, ESMA, 2024).

Gráfico 4
Resultados de la simulación, distribución del impacto

La escasez temporal de liquidez puede ser grande a nivel del sistema



Nota: Distribución del impacto resultante de los resultados de la simulación, basada en un escenario de estrés por un ciberincidente que interrumpe a uno de los 10 principales participantes (nodos) de la red de liquidación de repos de la UE. Simulación realizada durante 100 días seleccionados aleatoriamente, de enero de 2023 a junio de 2024. Indicadores de impacto calculados a nivel de sistema (entre las contrapartes de cada «nodo afectado»): déficit de liquidez en miles de millones de euros (panel a), número de entidades afectadas (panel b), porcentaje de endeudamiento afectado (panel c).
Fuente: SFTR, cálculo ESMA.

En segundo lugar, como se destaca, esta simulación de estrés utiliza información sobre nodos de asentamiento críticos, es decir, entidades que son participantes directos de los CSD y liquidan operaciones repo por cuenta propia o de sus clientes, para examinar otros posibles canales de contagio tras un incidente cibernético.

El gráfico 5 (panel c) muestra que, en una cuarta parte de los casos, las contrapartes afectadas toman prestado efectivo de entidades que dependen de un tercero para liquidar sus transacciones repo.

Los resultados también destacan que este canal puede transmitir shocks de liquidez significativos a través de

16 Un análisis de red realizado por la ESMA (2024) ilustra
La existencia de una estructura centro-periferia en el mercado de repos de la UE, que destaca el papel de intermediación de los bancos (en el núcleo) a través del cual diversas contrapartes de diferentes sectores acceden a la red de repos. Por diseño,
El segmento despejado centralmente muestra un patrón en forma de estrella. o más bien varios patrones en forma de estrella alrededor de varias CCP, con exposiciones significativas que fluyen a través de unas pocas
CCP principales y unos pocos miembros compensadores grandes.

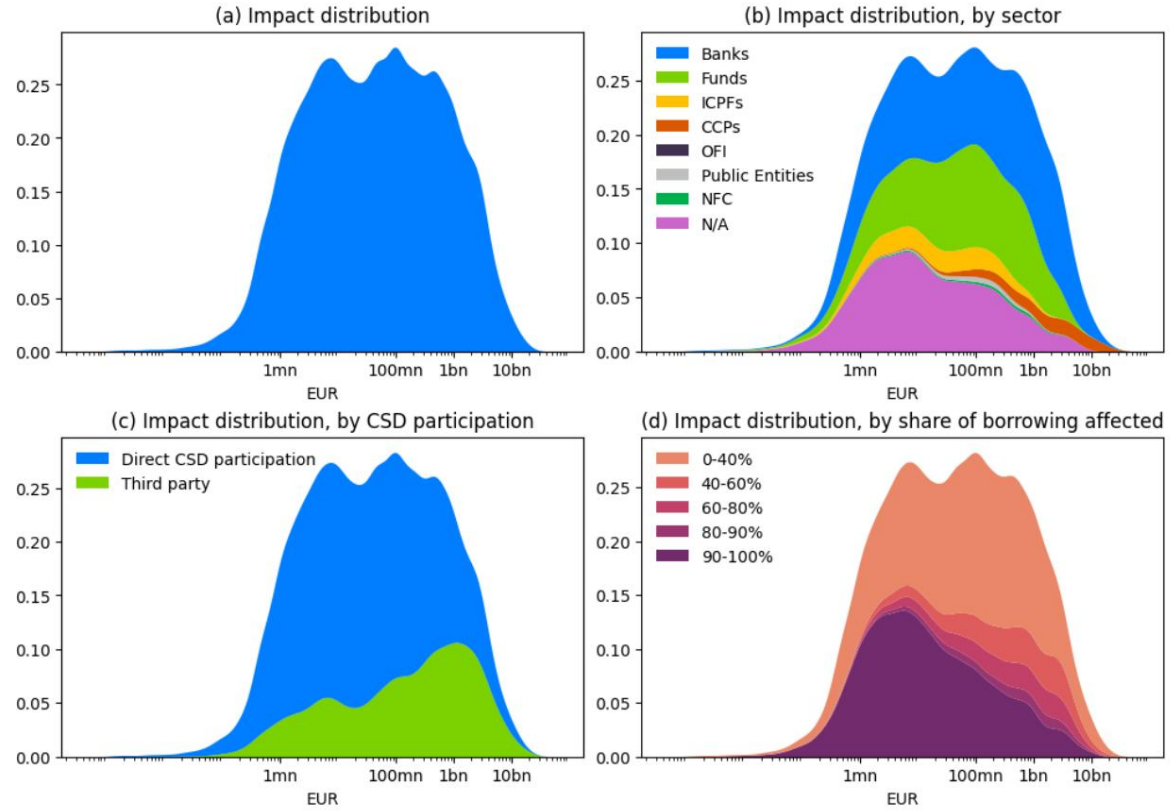
Machine Translated by Google

sistema: las contrapartes que reciben financiación de repos de entidades que dependen de la liquidación de terceros pueden experimentar una escasez temporal de liquidez de tamaño significativo (es decir, como lo ilustra el sesgo área verde ubicada prominentemente en el lado derecho del gráfico). Esto puede reflejar que
Las contrapartes que reciben financiación de varias entidades, pero a través de un nodo de liquidación compartido afectado por el ciberataque, probablemente experimentarán un gran impacto, ya que las operaciones de liquidación de todos estos prestamistas se verían afectadas.
por el mismo incidente. El análisis identifica así centros de asentamiento y dependencias de terceros como canales críticos de contagio.

En tercer lugar, si bien el impacto de la liquidez en entidades individuales puede ser significativo en términos absolutos, puede representar solo una pequeña proporción de la actividad total de repos de las contrapartes. Según nuestros resultados, cuando una contraparte se ve afectada por...
incidente, en el 25% de los casos el impacto afecta a menos del 9% del total de sus préstamos repo (véase el Cuadro 1).

Gráfico 5
Resultados de la simulación, distribución del impacto

Amplio impacto en todos los sectores y diferentes canales de contagio



Nota: Distribución del impacto de liquidez calculada a nivel de contraparte, resultante de una simulación de estrés en la que un ciberincidente afecta a uno de los 10 principales participantes de la red de liquidación de repos de la UE. El impacto se calcula en función del déficit temporal de liquidez que podrían afrontar las contrapartes en el escenario analizado y se calcula como la suma del total de los préstamos netos de repos afectados por el incidente (expresado en miles de millones de euros). La distribución del impacto se desglosa por contraparte.
sector (panel b), por participación directa o indirecta en los CSD (es decir, si el financiamiento de repos es provisto por prestamistas que dependen de terceros para proporcionar servicios de liquidación o no; panel c), según la proporción del endeudamiento de la empresa afectado por el evento (panel d).
Simulación realizada durante 100 días seleccionados aleatoriamente, desde enero de 2023 hasta junio de 2024.
Fuente: SFTR, cálculo ESMA.

La proporción limitada de la financiación total afectada por la disrupción puede indicar que las contrapartes cuentan con una amplia red de relaciones de repos para cubrir sus necesidades de financiación. En igualdad de condiciones, una red de repos más amplia puede aumentar la resiliencia ante las perturbaciones al permitir que las instituciones obtengan financiación de

Prestamistas de repos alternativos (a través de nodos de liquidación no afectados). El gráfico 5 (panel d) ilustra este punto con más detalle y muestra que, en general, cuanto mayor es el impacto en la liquidez, menor es la proporción de préstamos afectados (y viceversa). Este hallazgo sugiere que los participantes del mercado más grandes

Machine Translated by Google

Las empresas que enfrentan impactos potencialmente mayores tienden a contar con redes más amplias y fuentes de financiación de repos más diversificadas. Por otro lado, el resultado también sugiere que, en el caso de impactos menos significativos, por ejemplo, asociados con exposiciones más reducidas de empresas más pequeñas, la proporción de endeudamiento afectada por el incidente es, en cambio, alta, lo que presumiblemente refleja las redes de repos menos desarrolladas de algunas empresas que dependen de un número relativamente pequeño de intermediarios para cubrir sus necesidades de financiación.

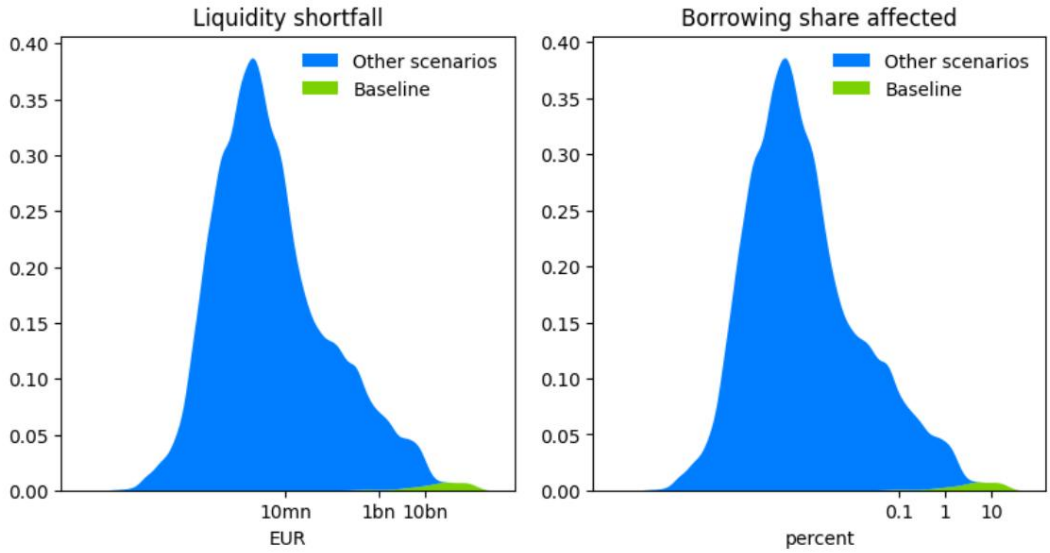
En principio, una evaluación integral de riesgos no debería centrarse únicamente en la magnitud del impacto potencial. Por ejemplo, las instituciones más grandes o sofisticadas podrían contar con más recursos, planes de contingencia o reservas para afrontar interrupciones temporales o déficits de liquidez.

que otros participantes del mercado. Factores como el tamaño de la institución, el sector, la solidez del balance, la planificación de contingencias, las prácticas de gestión de riesgos y los requisitos regulatorios también influyen en la evaluación de riesgos.

Prueba de esfuerzo inversa

Los resultados del análisis de simulación mostraron que un ciberataque exitoso en cualquiera de los 10 nodos de liquidación más grandes de la red de repos de la UE podría tener un impacto de gran alcance en el sistema. Como se destaca, estos nodos son generalmente grandes. instituciones que son participantes directos en los CSD y liquidan grandes volúmenes de operaciones repo en nombre propio o en nombre de sus clientes (como en el caso de los bancos custodios).

Gráfico 6
Prueba de esfuerzo inversa
Riesgos adicionales de los nodos de asentamiento “menos críticos”



Nota: Distribución del impacto de una simulación de estrés inverso, considerando un ciberincidente hipotético en cualquiera de los nodos de liquidación de la red de repos (incluidos los 10 nodos principales, es decir, el escenario base; área verde). Simulación de 100 días aleatorios (enero de 2023-junio de 2024). Déficit de liquidez calculado a nivel de sistema (escala logarítmica).
Fuente: SFTR, cálculo ESMA.

Estas grandes instituciones pueden beneficiarse de las economías de escala en la inversión en ciberseguridad y podrían estar sujetas a requisitos regulatorios más estrictos, lo que refuerza aún más sus defensas. En consecuencia, es probable que los ciberataques tengan más éxito cuando se dirigen a instituciones con marcos de seguridad más débiles, buscando vulnerabilidades más fáciles de explotar. Las instituciones más pequeñas podrían carecer de los amplios recursos necesarios para defenderse de ataques sofisticados, lo que las hace más vulnerables a las brechas de seguridad.

Se realizó una prueba de estrés inversa para evaluar si un ataque a nodos menos críticos de la red aún podría representar una amenaza significativa para la estabilidad financiera. Se realizó un conjunto más amplio de cálculos para cuantificar el posible déficit de liquidez resultante de un hipotético ciberataque dirigido a cualquiera de los nodos de liquidación del sistema.

El Gráfico 6 resume los resultados, ilustrando la distribución sistémica de los posibles déficits de liquidez causados por un ataque exitoso a cada nodo de la red de repos. Esta simulación inversa también considera las interrupciones en

Machine Translated by Google

los 10 nodos de asentamiento más grandes examinados previamente en el escenario de referencia, por lo que Ampliando el alcance del análisis. El impacto asociado a estos nodos se destaca en el área verde del Gráfico 6.

En el escenario base —donde un ataque se dirige a uno de los 10 nodos de liquidación más grandes—, los efectos adversos son más graves, como lo muestra el área verde en la cola derecha de la distribución del impacto. El análisis subraya que las interrupciones operativas en estos nodos críticos podrían provocar una escasez significativa de liquidez a nivel del sistema, lo que llevaría a resultados desfavorables.

Sin embargo, los ciberataques exitosos contra nodos de liquidación menos críticos también pueden tener consecuencias significativas. Por ejemplo, nuestros hallazgos indican que un incidente en un nodo que procesa menos de una décima parte del promedio de flujos liquidados por un nodo principal podría generar impactos sustanciales en la liquidez de todo el sistema, por un valor aproximado de 5000 millones de euros o más (aproximadamente el 1 % del total de préstamos repo en los escenarios analizados). Estos resultados ponen de relieve que incluso los ataques a pequeña escala pueden tener implicaciones sistémicas cuando se ven amplificados por la interconexión de la red.

Conclusión

El riesgo cibernético se ha convertido en una amenaza creciente para la estabilidad financiera. La frecuencia y la sofisticación de los incidentes han aumentado en los últimos años, y su impacto financiero es significativo y creciente.

La medición y el monitoreo de las ciberamenazas desde la perspectiva de la estabilidad financiera plantean desafíos considerables. El panorama de amenazas, dinámico y en rápida evolución, sumado a la limitada visibilidad de los incidentes, dificulta la evaluación precisa de riesgos. En Europa, se prevé que la Ley de Resiliencia Operativa Digital (DORA) tenga un impacto concreto en la visibilidad de los incidentes.

Introduce un marco armonizado y completo para la resiliencia operativa digital de las instituciones financieras de la UE y también establece un régimen de presentación de informes sobre los principales incidentes relacionados con las tecnologías de la información y la comunicación (TIC) cometidos por las instituciones financieras de la UE.

Este documento pretende contribuir a la arquitectura en evolución para la monitorización y evaluación del riesgo cibernético y operativo desde una perspectiva de estabilidad financiera. Se basa en el marco introducido por la ESMA en 2018, que reconoce las ciberamenazas como una categoría de riesgo diferenciada y en evolución que requiere un enfoque analítico específico.

Explora marcos conceptuales para examinar cómo los incidentes individuales pueden volverse sistémicos, centrándose en las exposiciones a las amenazas cibernéticas, la propagación del impacto a través del sistema y su impacto.

El documento también presenta los resultados de un análisis de simulación realizado en el mercado de repos de la UE, que sugiere que las interrupciones operativas en algunos participantes del mercado pueden provocar una escasez de liquidez temporal pero grave, tanto a nivel del sistema como de las contrapartes, con efectos de red generalizados. Estos mecanismos pueden amplificar el shock inicial y contribuir a una inestabilidad financiera más amplia.

Si bien todavía ningún incidente ha tenido un impacto significativo en el sistema financiero, el análisis ilustra cómo los shocks cibernéticos podrían evolucionar hacia riesgos más convencionales, como crisis de liquidez y perturbaciones del mercado, y tener consecuencias sistémicas.

Al integrar modelos conceptuales, simulaciones de estrés y métricas sistémicas, este documento ejemplifica el tipo de conjunto de herramientas analíticas previsto en ESMA (2018) y subraya el valor de estas metodologías para comprender, evaluar y medir mejor el riesgo cibernético.

Machine Translated by Google

Lecturas relacionadas

Brando, D., Kotidis, A., Kovner, A., Lee, M., Schreft, S., L. (2022), “Implicaciones del riesgo cibernético para “Estabilidad financiera”, Notas del FEDS.

Bouveret, A. (2019), “Estimación de pérdidas por riesgo cibernético para instituciones financieras”, Journal of Riesgo Operacional, vol. 14, no. 2 (junio), pp. 1-20.

Boston Consulting Group (BGC, 2019), “Global Wealth 2019: Reavivando el crecimiento radical”.

Centro de Estudios Estratégicos e Internacionales (2020), “Los costos ocultos del ciberdelito”.

Coste, C., Tcheng, C., Vansieleghem, I. (2021), “Una talla única: análisis de las restricciones de rentabilidad, capital y liquidez de los bancos custodios a través de la metodología SREP”, ECB Occasional Paper Series, n.º 256.

Duffie, D., Younger, J. (2019), “Cyber Runs”, Documento de trabajo inédito del Centro Hutchins 51, Institución Brookings.

Embroker (2024), "¿Cuánto cuesta una filtración de datos en 2024?".

Banco Central Europeo (BCE, 2024), “El BCE concluye la prueba de resistencia a la ciberresiliencia”, Nota de prensa.

Banco Central Europeo (BCE, 2025), “Pruebas de estrés de ciberresiliencia desde un punto de vista macroprudencial” perspectiva”, Boletín Macroprudencial del BCE, n.º 27.

Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2016), “El coste de los incidentes que afectan a las ICI”

Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2024), «Enisa Threat Landscape 2024»

Eisenbach, T., M., Kovner, A., Lee, M., J. (2021), “Riesgo cibernético y el sistema financiero estadounidense: un análisis pre-mortem”, Informes del personal del Banco de la Reserva Federal de Nueva York, n.º 90.

Comité Mixto de las Autoridades Europeas de Supervisión (ESA, 2024), “Borrador de normas técnicas reglamentarias y de ejecución sobre el contenido de los informes de incidentes graves de DORA”, Informe final.

Autoridad Europea del Mercado de Valores (ESMA, 2021), «Directrices», Informes con arreglo a los artículos 4 y 12 SFTR.

Autoridad Europea del Mercado de Valores (ESMA, 2024), “Mercados de transacciones de financiación de valores de la UE 2024”, Informe de mercado de la ESMA.

Autoridad Europea del Mercado de Valores (ESMA, 2018), “Evaluación del riesgo operativo: el enfoque de la ESMA”, Informe de la ESMA sobre tendencias, riesgos y vulnerabilidades n.º 1, 2018, págs. 68 y siguientes.

Junta Europea de Riesgo Sistémico (JERS, 2020), “Riesgo cibernético sistémico”, Tech. rep. European Systemic Risk Junta de Riesgos.

Junta Europea de Riesgo Sistémico (JERS, 2022), “Mitigación del riesgo cibernético sistémico”, Tech. rep. European Junta de Riesgo Sistémico.

Junta Europea de Riesgo Sistémico (JERS, 2023), “Avanzando en herramientas macroprudenciales para la ciberresiliencia”.

Junta Europea de Riesgo Sistémico (JERS, 2024), “Avanzando en las herramientas macroprudenciales para la ciberresiliencia – “Herramientas de política operativa”.

Consejo de Estabilidad Financiera (FSB, 2018), “Cyber Lexicon”.

Consejo de Estabilidad Financiera (FSB, 2020), “Prácticas efectivas para la respuesta y recuperación ante incidentes cibernéticos”.

Consejo de Estabilidad Financiera (FSB, 2021), “Informes de incidentes cibernéticos: enfoques existentes y próximos pasos para una convergencia más amplia”.

Financial Times (FT, 2024), “Un ataque de ransomware al ICBC interrumpe las operaciones en el mercado de bonos del Tesoro de EE. UU.”.

Fitch Ratings (FITCH, 2023), “El ciberataque a una subsidiaria estadounidense de ICBC destaca la interrupción de los pagos” “Riesgos”.

Machine Translated by Google

Healey, J., P. Mosser, K. Rosen, A. Wortman (2018), “Los lazos que unen: un marco para evaluar el vínculo entre los riesgos cibernéticos y la estabilidad financiera”, Proyecto sobre el riesgo cibernético para la estabilidad financiera, Escuela de Asuntos Internacionales y Públicos, Universidad de Columbia, Nueva York.

Centro de recursos sobre robo de identidad (2020), “Informe de violación de datos”.

Iyer, R., Macchiavelli, M. (2017), "La naturaleza sistémica de los fracasos en los acuerdos", Notas de la FEDS. Washington: Junta de Gobernadores del Sistema de la Reserva Federal, 3 de julio de 2017.

Moody's (2021), “El ataque Sunburst a entidades públicas y privadas aumenta los riesgos crediticios a medida que el alcance de

“Se despliega la brecha”, marzo de 2021.

Asociación Internacional del Mercado de Capitales (ICMA, 2023), “Una guía de mejores prácticas en el mercado europeo de repos”, noviembre de 2023.

Fondo Monetario Internacional (FMI, 2024), “Informe sobre la estabilidad financiera mundial”, abril de 2024.

Kaffenberger, L., Kopp, E. (2019), “Escenarios de riesgo cibernético, el sistema financiero y evaluación del riesgo sistémico”, Cyber Policy Initiative Working Paper Series, “Cybersecurity and the Financial System”, No. 4, Carnegie Endowment for International Peace, Washington, DC.

Kashyap, AK, Wetherilt, A. (2019), “Algunos principios para regular el riesgo cibernético”, AEA Pap. Proc., 109, págs. 482-487.

Reuters (2024), “Explicación: ¿Qué es Lockbit? El cierre de la banda digital tras una ola de ciberdelitos”.

Reuters (2023a), “Yellen: el hackeo a ICBC no tiene impacto en el mercado de bonos del Tesoro de EE. UU.”.

Reuters (2023b), “El revuelo en Wall Street tras el hackeo a ICBC”.

Ross, G. (2020), “La creación de un ciberaccidente: un modelo conceptual para el riesgo sistémico en el sector financiero”, Occasional Paper Series, n.º 16, mayo, Junta Europea de Riesgo Sistémico.

Statista (2022), “Se espera que la ciberdelincuencia se dispare en los próximos años”.

The Banker (2023), “La importancia del hackeo del ICBC FS en el mercado del Tesoro de Estados Unidos”.

Machine Translated by Google