Una triple amenaza en las Américas: KPMG 2022 Fraud Outlook

Sector destacado: servicios financieros

Cinco cosas que los ejecutivos de servicios financieros deben saber

En enero de 2022, **"Una triple amenaza en las Américas"** de KPMG destacó las amenazasde fraude, de incumplimiento y de ataques cibernéticos que enfrentan las empresas en todos los sectores en la actualidad. Este artículo de seguimiento analiza los peligros que enfrentan las empresas de servicios financieros (FS), y describe cinco cosas que los ejecutivos de FS deben saber:

01 Las firmas de FS tienen la carga de fraude más extensa y costosa de entre cualquier sector en las Américas.

El fraude es la norma y no la excepción en todas las industrias, pero lo es especialmente en la de servicios financieros. El 85% de los encuestados de FS informaron que sus empresas experimentaron al menos un fraude en el último año. Durante el mismo período, la pérdida generada por fraude en estas empresas fue equivalente al 0,6% de las ganancias anuales, una cuarta parte más que el promedio intersectorial de 0,48%.

El 85% de los encuestados de FS informaron que sus empresas experimentaron al menos un fraude en el último año.

02 Los *"insiders"*, los clientes y los delincuentes organizados representan una amenaza casi equivalente de fraude para las empresas de FS.

En lugar de una clase dominante de estafadores, las empresas de esta industria deben estar preparadas para las amenazas provenientes de cualquier dirección. Una fuente de estas amenazas está representada por los que están dentro de la propia empresa ("insiders"): el 34% de los encuestados de FS informan un fraude conocido en el último año perpetrado por uno o más ejecutivos sénior, gerentes intermedios o empleados operativos. Una cifra similar a los fraudes perpetrados por los clientes, que fue del 31%, y la asociada a aquellos fraudes cometidos por delincuentes organizados, incluidos los ciberdelincuentes.

De cara al futuro, la incidencia de estos riesgos podría empeorar: el 56% de los encuestados de FS espera que la amenaza de fraude de actores externos aumente el próximo año, en comparación con sólo el 17% que ve una disminución. Mientras tanto, el 69% de los ejecutivos cree que "el crimen organizado sigue siendo un desafío importante para hacer negocios legalmente" donde trabajan. Esto está muy por encima del promedio para todas las industrias, lo que sugiere un riesgo particularmente elevado.

03 Respecto del cumplimiento, que ya es un área difícil para las empresas de FS, se avisora que se volverá mucho más estricto.

Los costos del incumplimiento son actualmente altos para el sector. Los encuestados informan que, en promedio, sus empresas tuvieron que pagar el equivalente al 0,54% de las ganancias en multas durante el último año, muy por encima del promedio general, que fue del 0,46%. De cara al futuro, la mayoría de los ejecutivos de FS esperan que estas dificultades aumenten. El 62% piensa que el riesgo general de cumplimiento aumentará el próximo año, en comparación con sólo el 11% que prevé una disminución.

Nuevamente, en lugar de un solo problema, las amenazas de cumplimiento tomarán múltiples formas. En particular, el 61% de los líderes de la industria encuestados esperan enfrentar nuevos requisitos relacionados con la privacidad de datos y el 45% un aumento en la divergencia internacional de las reglas sobre anticorrupción y antilavado de dinero, temas particularmente relevantes para los proveedores de servicios financieros transfronterizos.

Mientras tanto, después del cierre de esta encuesta, los eventos geopolíticos en Ucrania complicaron aún más el cumplimiento de FS en particular. Estados Unidos juega un papel crítico en proporcionar la infraestructura para el sistema financiero global. Como resultado, sus amplias y recientemente sanciones impuestas son ahora, en la práctica, requisitos para casi todas las empresas del sector. También serán reglas en las que - de no cumplirlas- los riesgos regulatorios y reputacionales serán muy altos.

04 Las empresas de FS están experimentando una variedad de impactos negativos debido a una ola de nuevos riesgos cibernéticos.

En el último año, el 87% de las empresas de la industria vieron un aumento de al menos un tipo de ataque cibernético, la cifra más alta en nuestra encuesta para cualquier sector. El phishing (reportado por el 49%) y la estafa (37%) experimentaron el crecimiento más generalizado, pero más de uno de cada cinco (21%) negocios de servicios financieros está lidiando con un número creciente de ataques de ransomware. El daño resultante no es sólo económico: el 31% de los ejecutivos de la encuesta dicen que un ataque cibernético desencadenó una investigación regulatoria o de cumplimiento en su empresa durante los últimos 12 meses, y casi una cuarta parte (23%) que tal evento de TI condujo a una investigación sostenida de daño reputacional.

Aquí, también, se vislumbra poco/insuficiente respiro: el 78% espera que aumenten los riesgos cibernéticos. Mientras tanto, se espera que la Comisión de Bolsa y Valores de EE. UU. apruebe un requisito de notificación de cuatro días para incidentes cibernéticos, lo que aumenta aún más el riesgo regulatorio concomitante.[1]

[1] "Gestión de riesgos de ciberseguridad, estrategia, gobernanza y divulgación de incidentes", Norma propuesta, 9 de marzo de 2022, HIPERVÍNCULO "https://www.sec.gov/rules/proposed/2022/33-11038.pdf" https://www. .sec.gov/rules/proposed/2022/33-11038.pdf

05 Frente a esta triple amenaza sustancial, muy pocas empresas piensan que tienen defensas sólidas y muchas revelan vulnerabilidades.

Si bien la triple amenaza que enfrenta la industria de FS es incluso mayor a la que enfrentan otros sectores, muchas empresas carecen de los altos niveles de protección necesarios. Sólo el 58% cree que la seguridad de la red de su empresa es algo o muy madura, por ejemplo, mientras que el 31% dice que son extremadamente efectivos para encontrar instancias de fraude o incumplimiento y para tomar medidas para mitigar los efectos de ambos. Las defensas moderadamente buenas simplemente no son suficientes aquí.

Mientras tanto, las respuestas individuales dan una pausa para pensar. A más de la mitad de los encuestados de FS (53%), por ejemplo, no les sorprendería saber que el próximo año se filtraron datos privados de clientes de su empresa; en tanto que el 61% informa que no ha actualizado efectivamente los controles de fraude vigentes previo a la pandemia para reflejar la nueva realidad laboral, y slo el 43% espera aumentar la inversión en mejorar el cumplimiento en el próximo año, a pesar del creciente riesgo de incumplimiento y el ya alto costo para el sector. Asimismo, el 28% piensa que sus empresas pagarían a quienes están detrás de un ataque de ransomware si ocurriera uno, la cifra más alta para cualquier industria. Dado el alcance actual de la triple amenaza, se aprovecharán las debilidades específicas.

Punto de vista de KPMG: haga que sus defensas se ajusten a su propósito

El mundo siempre está cambiando, pero, de vez en cuando, experimenta un punto de inflexión dramático. La pandemia de COVID-19 restableció todo tipo de suposiciones sobre cómo vivimos y trabajamos. Ahora, los eventos geopolíticos están exponiendo las fragilidades de nuestras suposiciones sobre el entorno internacional.

El panorama de riesgos al que se enfrentan las empresas se ha remodelado de manera similar. La necesidad de mantener el acceso a los suministros ha llevado a muchas empresas a depender de socios que antes no habían sido investigados, lo que podría generar nuevos riesgos de fraude. En cuanto al cumplimiento, el impulso por el cero neto creará una mayor regulación ambiental y las nuevas sanciones globales pueden conducir a una supervisión más estricta de la actividad financiera y comercial. Finalmente, los ataques cibernéticos, que ya aumentaron durante la pandemia, están permitiendo a los actores de amenazas cibernéticas perseguir una variedad de objetivos.

En resumen, si su empresa no ha realizado recientemente una revisión completa de sus riesgos de fraude, cumplimiento y ciberseguridad, debe realizarla lo antes posible. De lo contrario, sus defensas no estarán diseñadas para combatir las amenazas actuales, ni podrán reaccionar a medida que esos riesgos evolucionen rápidamente.

Si bien reexaminar los riesgos es una necesidad para todos los sectores, lo es especialmente para las empresas de FS. En tiempos de dificultad económica, con una inflación más alta que en muchos años, es mucho más probable que las personas dentro y fuera de las empresas racionalicen la participación en el fraude. FS será un objetivo principal para tales actores por la misma razón por la que ya sufre pérdidas descomunales: estos delitos tienen una motivación financiera, y FS es el sector donde la mayor parte del dinero es el foco del negocio.

El marco básico de prevención, detección y respuesta sigue siendo la base más sólida para abordar la triple amenaza del fraude, el incumplimiento y el ataque cibernético. Sin embargo, el entorno en el que se implementan estas defensas significa que deben conservar los elementos más efectivos y aprovecharlos para vencer las amenazas en evolución.

Prevención

Ciertos elementos permanecerán prácticamente iguales, como la implementación o mejora de los controles internos; diligencia debida de integridad basada en riesgos sobre empleados y terceros; evaluaciones de seguridad de sistemas de información críticos; y ataques cibernéticos simulados para exponer vulnerabilidades explotables. Otros tomarán una nueva forma. Por ejemplo, puede ser necesario implementar reglas sobre excepciones a las políticas de diligencia debida del proveedor en medio de la escasez de la cadena de suministro, pero las empresas deben equilibrar la necesidad estratégica con el imperativo de evitar ser víctima de fraude y mantenerse en el lado correcto de la regulación.

Detección

Las herramientas como el análisis de datos, las auditorías internas y los protocolos de detección de intrusos cibernéticos seguirán siendo fundamentales, pero los malos comportamientos que buscan pueden ser diferentes. Además, incluso cuando hay más empleados trabajando en casa, sus ojos y oídos son los que verán las fallas de cumplimiento o el fraude. Las medidas que las empresas deben tomar incluyen capacitación actualizada sobre riesgos de fraude y cumplimiento, y sobre la importancia de informar comportamientos inusuales a través de los mecanismos existentes de informe de incidentes.

Respuesta

Deben existir protocolos para responder al fraude, instancias de incumplimiento e infracciones cibernéticas. Las empresas también deben estar preparadas para los desafíos emergentes dentro del triángulo de riesgo actual. Esto podría incluir, por ejemplo, decidir con anticipación si está dispuesto a pagar en caso de que lo ataque un ransomware o elegir de antemano quién haría esa llamada.

Contactos:

Marc Miller
Partner, Advisory
Head of Risk and Compliance
KPMG US

Ivan Velez-Leon
Managing Director, Advisory
Forensics
KPMG US

Ana Lopez Espinar
Partner, Advisory
Co-Lead, Forensic Practice South America*
KPMG Argentina

Emerson Melo
Partner, Advisory
Co-Lead, Forensic Practice South America*
KPMG Brazil

Luis Preciado
Lead Partner
Risk Advisory Solutions
KPMG Mexico

kpmg.com/socialmedia