Una triple amenaza en las Américas: 2022 KPMG Fraud Outlook

Lo más destacado del sector: servicios financieros

Cinco cosas que el liderazgo de servicios financieros debe conocer

Una triple amenaza en las Américas. 2022 KPMG Fraud Outlook destacó los desafíos de fraude, incumplimiento y ataques cibernéticos que actualmente enfrentan las empresas de todos los sectores.
Este artículo de seguimiento analiza los peligros que encaran las compañías de servicios financieros (SF) y describe cinco aspectos que la Alta Dirección de esta industria debe conocer:

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

El fraude es la norma y no la excepción en diversos casos, pero lo es especialmente en los servicios financieros. La gran mayoría de los encuestados de SF (85%) informaron que sus empresas experimentaron al menos un fraude en el último año. Durante el mismo periodo, la pérdida conocida por fraude de estas organizaciones fue equivalente a 0.6 % de las ganancias anuales, una cuarta parte más que el promedio intersectorial de 0.48 %.

"La gran mayoría (85%) de los encuestados de SF reportan que sus compañías han experimentado al menos un fraude en el último año."

02 Los informantes, los clientes y el crimen organizado representan amenazas de fraude casi iguales para las empresas de SF

Más que concentrarse en una clase dominante de estafadores, las empresas de esta industria deben estar preparadas para las amenazas que vienen de casi cualquier lugar. Una fuente son los que están dentro de la propia compañía: 34% reporta que tuvoconocimiento de un fraude en el último año perpetrado por uno o más ejecutivos sénior, gerentes de nivel medio o empleados operativos. Casi tan generalizada es la amenaza de los clientes, que estaban implicados en el fraude en 31% de estas empresas. La misma proporción fue atacada por la delincuencia organizada, la cual incluye a los cibercriminales.

De cara al futuro, el entorno de amenazas podría empeorar: 56% de las empresas de este sector esperan que el fraude de actores externos aumente el próximo año, en comparación con solo 17% que ve una disminución. Mientras tanto, 69% del liderazgo cree que, donde trabaja, "el crimen organizado sigue siendo un desafío importante para hacer negocios". Esto está muy por encima del promedio, lo que sugiere un riesgo particularmente elevado.

03 Parece que el cumplimiento, que ya es un área difícil para las compañías de servicios financieros, se volverá mucho más estricto

Actualmente los costos del incumplimiento son altos para el sector. Los encuestados informan que, en promedio, sus empresas tuvieron que pagar el equivalente a 0.54% de las ganancias en multas durante el último año, muy por encima del promedio de 0.46 % de las diversas industrias. De cara al futuro, la mayoría de la Alta Dirección espera que estas dificultades aumenten; 62% piensa que el riesgo general de cumplimiento incrementará el próximo año, en comparación con solo 11% que prevé una disminución.

Nuevamente, en lugar de un solo problema, las amenazas de cumplimiento tomarán múltiples formas. En particular, 61% del liderazgo de la industria espera enfrentar nuevos requerimientos relacionados con la privacidad de datos y 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 internacionales.

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

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

En el último año, 87% de las organizaciones de la industria vieron un aumento de al menos un tipo de ciberataque, la cifra más alta en nuestra encuesta para cualquier sector. El *phishing* (reportado por 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 resultado es un daño no solo económico: 31% dice 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 tecnologías de la información (TI) condujo a un daño reputacional constante.

Aquí, también, se vislumbra un pequeño contratiempo: 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 de cumplimiento regulatorio.[1]

1 *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Norma propuesta, 2022.

05 Frente a esta triple amenaza sustancial, muy pocos negocios piensan que tienen defensas sólidas y muchas revelan vulnerabilidades

Si bien la triple amenaza que enfrenta la industria de servicios financieros es incluso mayor que la que encaran otras empresas, muchas carecen de los altos niveles de protección necesarios. Solo 58% cree que la seguridad de la red de su compañía es algo o muy madura, por ejemplo, mientras que solo 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 en este caso.

Mientras tanto, las respuestas individuales llaman la atención. A más de la mitad del liderazgo de servicios financieros (53%), por ejemplo, no le sorprendería saber que el próximo año se filtraran datos privados de clientes de su empresa; 61% informa que no ha actualizado efectivamente los controles de fraude previos a la pandemia para reflejar la nueva realidad laboral; solo 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; y 28% piensa que sus compañías 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.

Perspectiva 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 nos llevó a cuestionarnos las suposiciones que teníamos sobre cómo vivimos y trabajamos. Ahora, los eventos geopolíticos están exponiendo las fragilidades de nuestras suposiciones sobre el entorno internacional.

En la actualidad, el panorama de riesgos al que se enfrentan las empresas se ha reconfigurado de manera similar. La necesidad de mantener el acceso a los suministros ha llevado a muchas organizaciones 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 *net zero* 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 habían aumentado durante la pandemia, están permitiendo a los actores de amenazas cibernéticas perseguir una nueva 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 cuanto antes. De lo contrario, sus defensas no estarán diseñadas para combatir las amenazas actuales ni podrá reaccionar a medida que esos riesgos evolucionen.

Si bien reexaminar los riesgos es una necesidad para todos los sectores, lo es especialmente para las empresas de servicios financieros. En tiempos de dificultad económica, con una inflación más alta que en otros años, es mucho más probable que las personas dentro y fuera de las organizaciones racionalicen el participar en un fraude. SF 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 este 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, tales como la implementación o mejora de los controles internos, la diligencia debida de integridad basada en riesgos sobre empleados y terceros, las evaluaciones de seguridad de sistemas de información críticos, y los 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 *vendor due diligence* 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

Herramientas como el análisis de datos, las auditorías internas y la detección de intrusiones cibernéticas seguirán siendo fundamentales, pero los malos comportamientos que buscan pueden ser diferentes. Además, incluso cuando hay más empleados y empleadas trabajando en casa, sus ojos y oídos son los que verán las fallas de cumplimiento o los riesgos de fraude.

Las medidas que las empresas deben tomar incluyen capacitación actualizada sobre los riesgos, así como sobre la importancia de informar comportamientos inusuales utilizando los mecanismos existentes de informe de incidentes.

Respuesta

Deben existir protocolos eficaces para responder a situaciones de fraude, así como instancias para atender el incumplimiento y las infracciones cibernéticas. Las compañías deben prepararse para atender los desafíos emergentes dentro del triángulo de riesgo actual. Esto podría incluir, por ejemplo, decidir con anticipación si están dispuestas a pagar en caso de que las ataque un *ransomware* o elegir de antemano quién se hará responsable.

Para obtener más información sobre cómo KPMG puede ayudarle, contáctenos:

Marc Miller
Socio de Asesoría para las Américas* y Líder de Forensic de KPMG en Estados Unidos

Iván Vélez-León
Director Ejecutivo de Asesoría Forense de KPMG en Estados Unidos

Ana López Espinar
Socia de Asesoría y Colíder de la Práctica de Forensic en Sudamérica* y de KPMG en Argentina

Emerson Melo
Socio de Asesoría y Colíder de la Práctica de Forensic en Sudamérica* y de KPMG en Brasil

Luis Preciado
Socio Líder de Risk Advisory Solutions para KPMG en México y Centroamérica

Carlos Fernández
Socio Líder de Servicios Financieros para KPMG en México y Centroamérica

kpmg.com.mx KPMG MÉXICO @KPMGMEXICO KPMG MÉXICO KPMGMX