Una triple amenaza en las Américas: KPMG 2022 Fraud Outlook

Sector destacado: energía y recursos naturales

Cinco cosas que los ejecutivos de energía y recursos naturales deben saber

En enero de 2022, **"Una triple amenaza en las Américas"** de KPMG destacó los desafíos de 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 energía y recursos naturales (ENR), y describe cinco cosas que los ejecutivos del sector deben saber:

01 Es menos probable que las empresas de energía y recursos naturales informen sobre fraudes que las de otros sectores, pero también es posible que simplemente pasen por alto a cierto número de perpetradores.

La magnitud del problema del fraude en el sector ENR puede interpretarse de diferentes maneras. Un optimista señalaría que el 62% de las empresas de la industria que experimentaron un fraude en los últimos doce meses está cómodamente por debajo del promedio de la encuesta (71%). Un realista señalaría que una mayor frecuencia de delitos en otros lugares no cambia el problema de que el fraude sigue siendo la norma, no la excepción, en las empresas de energía y recursos naturales. Las cifras del costo económico promedio del fraude brindan menos consuelo a los ejecutivos esperanzados. Las empresas de ENR, en promedio, perdieron el 0,45% de las ganancias por estos delitos en los últimos 12 meses, muy cerca de la cifra general de la encuesta (0,48%). Esto sugiere que, aunque sean menos frecuentes, los fraudes contra las empresas de energía y recursos naturales suelen ser más costosos que los de otras industrias.

Una preocupación final sobre los niveles de fraude que afectan al sector es que sus empresas pueden atrapar una proporción menor de delincuentes que las empresas de otras industrias. Por ejemplo, las empresas de ENR fueron las menos propensas a informar haber encontrado un fraude a través de una auditoría interna en los 12 meses anteriores (26% en comparación con el 34 % general), pero lo más probable es que dijeran que una auditoría externa reveló alguno (21% vs. 14%). Del mismo modo, sólo el 17 % de los encuestados de ENR dijeron que el análisis de datos reveló algún fraude el último año, el más bajo para cualquier sector y muy por debajo del promedio de la encuesta, que fue del 27%.

Es difícil estar seguro, pero, en cualquier caso, si la actividad ilícita no está ocurriendo o simplemente no se ha descubierto, estos datos hacen que esta última posibilidad sea una preocupación importante.

02 La complacencia en torno al fraude es un peligro entre las empresas de energía y recursos naturales. Las respuestas de la encuesta de esta industria revelan una preocupación insuficiente por el riesgo de fraude.

Por ejemplo, mientras que el 76% de los encuestados de energía y recursos naturales considera que los planes de respuesta al fraude de su empresa son algo o extremadamente efectivos, sólo el 45% incluye un elemento de respuesta en sus programas antifraude. Esta última es la cifra más pequeña para cualquier sector. En otras palabras, al menos el 31% dice que los esfuerzos inexistentes son algo efectivos.

Más sorprendente, el 74% de los encuestados de energía y recursos naturales cree que en el próximo año aumentará el riesgo de fraude por parte de perpetradores dentro de la empresa, fuera de la empresa o ambos. Esta es la segunda cifra sectorial más alta (después del 76% obtenido por "ciencias de la vida") y notablemente más alta que el promedio de la encuesta, que fue del 66%. Mientras tanto, el 67% informa que "los controles antifraude que teníamos antes de la pandemia no se han actualizado de manera efectiva para reflejar la nueva realidad laboral". Esa es la proporción más alta para cualquier industria. La necesidad clara, entonces, es la de articular mejores defensas, pero sólo el 38% de los encuestados de energía y recursos naturales espera que la inversión corporativa en medidas antifraude aumente el próximo año, siendo la cifra más baja en un sector, y en marcado contraste con el promedio de la encuesta, que fue del 53%.

Esta combinación de actitudes exacerba el riesgo. Uno de los peores escenarios para el fraude se da cuando los empleados reconocen la ausencia de inversión en controles. Aquellos que puedan racionalizar la participación en el fraude, un número creciente en medio de la alta inflación en muchos países, verán una oportunidad.

03 Los riesgos de fraude específicos para el sector parecen venir, literalmente, con el territorio.

A pesar de que las cifras generales de fraude están por debajo del promedio, las empresas de energía y recursos naturales son las más afectadas por dos tipos específicos de delitos: el 18% de las empresas del sector sufrieron fraude de vendedores/proveedores en el último año. El promedio de la encuesta fue sólo del 13%. Del mismo modo, el soborno salió a la luz en el 13% de las empresas de la industria, frente a sólo un 9% en general.

Estos esquemas de fraude específicos pueden reflejar un atributo asociado a la actividad de energía y recursos naturales. Las empresas deben operar siempre que sea posible extraer el producto, lo que limita su capacidad para elegir entornos con menores riesgos de fraude. Al no poder cambiar de ubicación, las buenas defensas contra el fraude constituyen la única opción viable para la industria.

04 El cumplimiento ambiental, una preocupación creciente y de alto perfil para las empresas de energía y recursos naturales, está recibiendo atención.

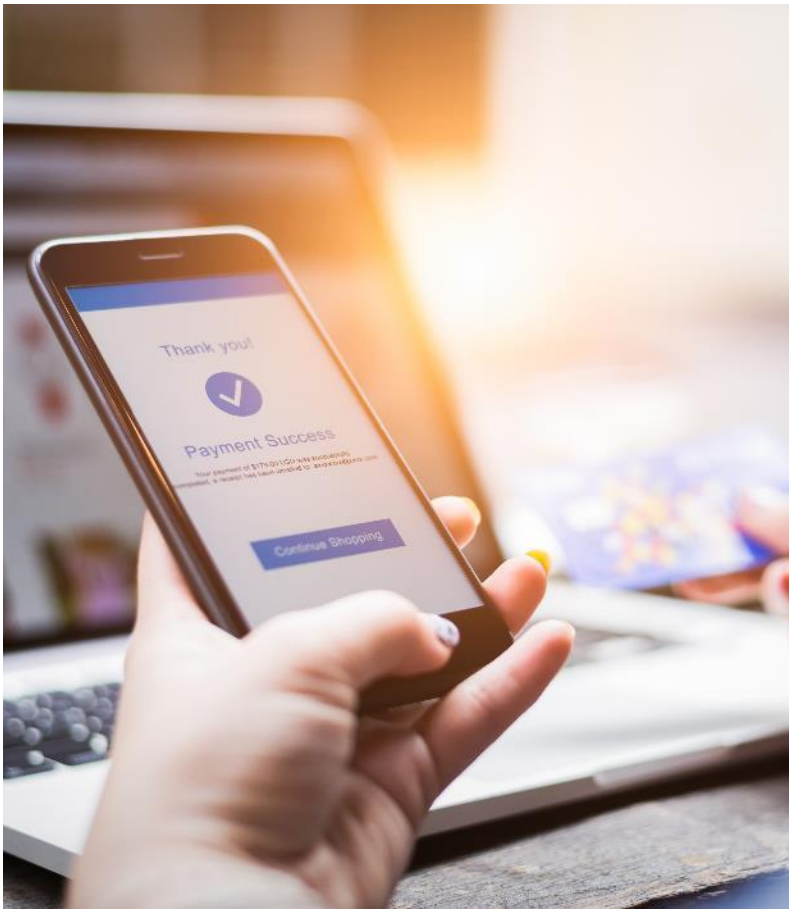
Estos encuestados son los más propensos de cualquier sector a esperar que los nuevos requisitos regulatorios o de cumplimiento ambiental los afecten en los próximos cinco años (54% en comparación con el 47% en general). En el lado positivo, los programas de cumplimiento ambiental de la industria tienen muchas más probabilidades que el promedio de seguir las mejores prácticas internacionales: el 31% de los encuestados del sector dice que sus empresas cumplen con este estándar, en comparación con sólo el 21% en general.

Es una pregunta abierta si ésta cifra es lo suficientemente alta, teniendo en cuenta que las industrias extractivas en particular están asociadas con huellas ambientales altas. Para estas empresas, su licencia metafórica y real para operar está ligada a sólidos programas de cumplimiento: el 85% de los expertos en ENR informan que los riesgos reputacionales están causando que el liderazgo en su empresa preste una atención sustancial o mayor a los problemas de cumplimiento; el 80% dice lo mismo de una aplicación más rigurosa; y 80%, nuevamente, respecto a las demandas por parte de clientes o proveedores. La mayoría de las empresas de la industria están jugando a lo seguro: el 53% espera aumentar el gasto en cumplimiento normativo general el próximo año, la cifra más alta del sector.

05 La ciberseguridad es otro campo en el que el aparente exceso de confianza es un peligro.

Esto va más allá del nivel generalmente creciente de riesgo cibernético que enfrentan todas las empresas. Las empresas del sector, en particular las de energía, son objetivos particularmente tentadores para los piratas informáticos en este momento, tanto por sus activos monetarios como por la infraestructura crítica que brindan a las sociedades.

Dado este entorno de riesgo preocupante para la industria, otras respuestas parecen revelar un exceso discordante de confianza en sí misma. Para empezar, el 87% de los ejecutivos de ENR dice que los controles de la empresa para evitar la pérdida de datos por errores de los empleados son algo o muy efectivos, lo que hace que esta sea la respuesta más confiable del sector a esta pregunta. Mientras tanto, al 51% de esos mismos encuestados no les sorprendería enterarse de una fuga de datos de clientes. Más llamativo, el 86% está algo o completamente satisfecho con la rapidez con la que sus empresas pueden identificar ataques a su sistema informático, pero sólo el 21% de estas empresas pueden hacerlo en una semana o menos, la cifra más baja del sector.



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.

El sector ENR se enfrenta a nuevas amenazas urgentes para las que debe estar preparado. Por ejemplo, las empresas del sector, en particular las de energía, son objetivos especialmente tentadores para los piratas informáticos, tanto por sus activos financieros como porque brindan infraestructura crítica a las sociedades. KPMG ha visto evidencia de malos actores que buscan identificar a personas dentro de estas organizaciones que podrían estar dispuestas a ayudarlos a obtener un punto de apoyo digital.

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.

Para algunas empresas de energía y recursos naturales, esto puede requerir un cambio de rumbo difícil. Durante la pandemia, los precios más bajos hicieron que las empresas de energía en particular se redujeran. Esto, a su vez, condujo a un mayor énfasis en los negocios cotidianos y un enfoque reducido en los controles antifraude y las auditorías internas. Los resultados de nuestra encuesta destacan repetidamente la pobre eficacia resultante del control de seguridad cuando se descuidan estas medidas. Con la recuperación de los precios, no hay excusas para no abordar la triple amenaza de manera agresiva.

Para aquellos que estén listos para hacerlo, el marco básico de prevención, detección y respuesta sigue siendo la base más sólida para abordar el fraude, el incumplimiento y los ataques cibernéticos. 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

Herramientas como análisis de datos, auditorías internas y los protocolos de detección de intrusiones cibernéticas seguirán siendo fundamentales, pero las malas conductas 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 los riesgos de fraude y cumplimiento, y sobre la importancia de informar comportamientos inusuales a través de los mecanismos existentes de notificación de incidentes.

Respuesta

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