La importancia del Seguro de Crime y/o Actos Fraudulentos en Época del Covid-19.

15 mayo, 2020

LOCKTON®

La importancia del Seguro de Crime y/o Actos Fraudulentos en Época del Covid-19.

“Este seguro protege a las empresas contra actos fraudulentos o deshonestos, cometidos por empleados o terceros, con la intención de causar una pérdida o de obtener un beneficio financiero”

Entorno Actual

Las cuotas de las primas del seguro de Crime se encuentran a la alza mientras los delincuentes de este segmento explotan nuevas oportunidades creadas por la pandemia del COVID-19.

Los negocios deben estar seguros respecto de que han implementado las medidas de seguridad apropiadas y que son seguidas por sus colaboradores en la organización, sobretodo porque después de la recesión económica esperada después del brote es muy probable que las cuotas de del seguro de Crime incrementen aún más.

Después de la implementación de las medidas de cuarentena y distanciamiento social para contener la pandemia, las economías estrangularon la producción y servicios en todo el mundo. En consecuencia, el Fondo Monetario Internacional (FMI) pronostica que la economía global se contraerá un 3% en 2020.

Además de los resultados negativos en el corto plazo de los mercados laborales, las recesiones usualmente conllevan un incremento en actividad criminal.

Nuevos esquemas de fraude que los criminales están adaptando

Los criminales han sido rápidos en aprovechar oportunidades para explotar los esfuerzos de los gobiernos para combatir la propagación del coronavirus adaptando su modus operandi o involucrándose en nuevas actividades criminales.

De acuerdo con agencias internacionales de inteligencia, los factores que están detonando cambios en estos crímenes incluyen:

- Reducción en la movilidad y flujo de personas;
- Las limitaciones de la vida pública hacen que algunas actividades criminales sean más visibles y las desplazarán a realizarse desde casa o en línea;
- Personas que permanecen en casa y que cada vez más, trabajan de forma remota confiando en las soluciones digitales;
- Disminución de suministro de ciertos bienes ilícitos.

Mientras que el fraude tradicional como el robo de fondos por parte de colaboradores no ha desaparecido, el fraude electrónico por parte de terceros ha estado

aumentando exponencialmente en los años recientes, tanto en frecuencia como en severidad. Un esquema de fraude popular involucra la suplantación de personalidad para detonar una transferencia de fondos errónea, también conocida como ingeniería social y ha probado tener más efectividad durante este encierro de emergencia. Por ejemplo, es más fácil suplantar la personalidad de un socio corporativo si un nuevo proveedor ha sido recientemente seleccionado sin haber tenido una reunión de forma física debido a la situación que prevalece.

Los ciberdelincuentes están también explotando el hecho de que un mayor número de colaboradores se conectan a los sistemas de las organizaciones de forma remota y creando potencialmente brechas de seguridad.

Además, los defraudadores han adaptado esquemas de fraude conocidos para capitalizar las ansiedades y miedos que la gente pudiera haber desarrollado debido a la crisis, incluyendo esquemas de fraude telefónico, estafa en suministro y estafas en descontaminación. Por ejemplo, en Europa se dio un incidente donde una compañía transfirió €6.6 millones a una compañía en Singapur para comprar alcohol en gel y cubrebocas. Los bienes jamás se recibieron.

Los esquemas fraudulentos que involucran robos también han sido adaptados por criminales para explotar la situación actual, incluyendo estafas que involucran robo de identidad de representantes legales o autoridades públicas. Se espera que las entidades comerciales o instalaciones médicas sean objetivos para robos organizados. Dado que muchas oficinas y plantas de manufactura están desocupadas, es esencial que se tanto la administración de cada ubicación como las medidas de seguridad sean más estrictas.

Medidas de seguridad adicionales

Ya que los procesos y la cooperación entre socios comerciales podrían haber cambiado durante la pandemia, las compañías deben tener especial cuidado al transferir fondos e introducir medidas adicionales de seguridad.

Entre las medidas que vale la pena revisar está educar al staff en ingeniería social y técnicas de fraude así como capacitar a los empleados en medidas de seguridad necesarias al realizar transferencia de fondos.

Ahora que la mayor parte de los colaboradores de diversas organizaciones están trabajando desde casa, los métodos de autentificación multi- factor son particularmente importantes ya que requieren que el usuario presente dos o más piezas de evidencia para obtener el acceso a un sistema. La seguridad de las computadoras de los colaboradores (personales) y en las redes domésticas usualmente se encuentra fuera del control de sus empresas. Dependiendo de cómo se esté accediendo a las redes del corporativo, si la computadora de uno de sus empleados contiene “malware” lo podría transmitir a la red de la compañía.

En abril, el proveedor de servicios de prevención de fraudes “Cifas”, reportó un enorme pico de actividad en línea alrededor del coronavirus, incluyendo un incremento en correos fraudulentos de personas haciéndose pasar por CEO’s o empleados del departamento de IT preguntando a los empleados por sus claves de acceso para compartir información de su pantalla.

Un endurecido mercado de Seguro de Crime

La póliza de seguro de Crime protege al asegurado de pérdidas financieras por actos fraudulentos “internos” y “externos”. Sin embargo, el apetito de los aseguradores para este tipo de riesgos ha disminuido en años recientes dado que la frecuencia y severidad de las reclamaciones han incrementado, particularmente en el robo de identidad y desvío de fondos. La reducción de la capacidad de suscripción se ha visto reflejada en primas y condiciones de las pólizas.

Algunos aseguradores ahora están sólo suscribiendo riesgos en coaseguro, compartiendo la exposición con al menos otros dos aseguradoras. Además, cuando las

compañías de seguros se sienten incómodas con el nivel de control corporativo de la compañía, podrían pedirle al mismo asegurado que retenga parte del riesgo. No es inusual ver compradores de la póliza de Crime a nivel global reteniendo el 50% de una posible reclamación cuando las medidas de seguridad varían entre distintas unidades de negocios.

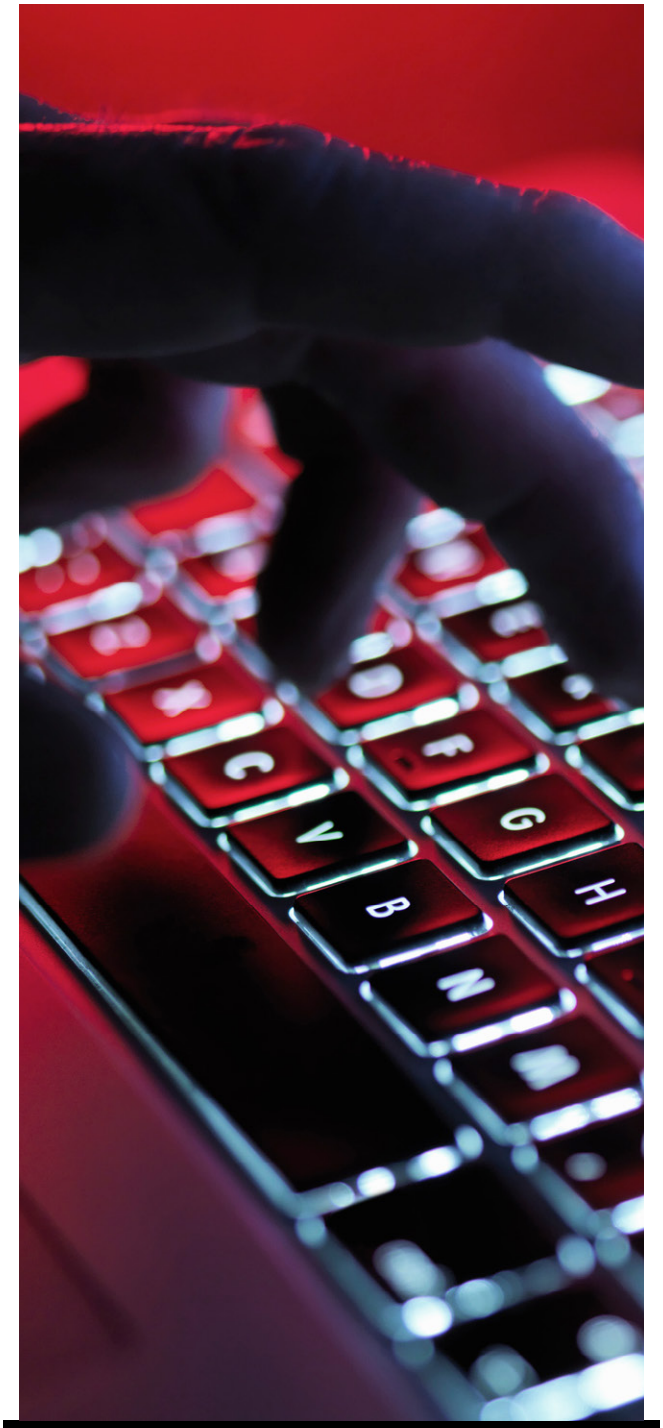
Los aseguradores de Crime están incrementando las retenciones (deducibles principalmente) de la póliza de forma significativa. Mientras que se espera que estas medidas mejoren los resultados de los suscriptores, supuestamente deberían incrementar el rigor de los controles y procedimientos de las compañías para incrementar la atención que se da a la mitigación de fraudes.

Es ahora normal que las pólizas de Crime tengan deducibles de USD25,000 y para compañías con ingresos de más de un billón, los deducibles están el orden de USD 1 millón o más.

El mercado del seguro de Crime es relativamente pequeño y de ahí que una pérdida pueda tener un gran efecto en el segmento. Algunas aseguradoras están suscribiendo la póliza de Crime para clientes ya existentes o que estén comprando otros productos, pero no están suscribiendo Crime solamente. Algunos otros mercados (reaseguradores), detuvieron la suscripción.

Las aseguradoras que continúan con la suscripción de este segmento no sólo están ajustando primas a los nuevos niveles de percepción del riesgo, también están solicitando más información acerca de los controles internos que los negocios tienen implementados contra fraude.

Como los criminales siguen el camino de menos resistencia y tienen como objetivo los firewalls más débiles, los aseguradores quieren ver evidencia de que el nivel de control es riguroso en todas las subsidiarias, que el mismo software para adquisiciones de bienes, productos y servicios es implementado a nivel global, que la auditoría de la compañía está centralizada y que las medidas de seguridad tales como la llamada de verificación, se realizan antes de haber concretado una transferencia de fondos.



Para mayor información contacta a:

Félix Leguízamo | Subdirector Daños

fleguizamo@mx.lockton.com

UNCOMMONLY INDEPENDENT