Fraude interno
en la industria del petróleo

Por ***Martín Elizalde***, socio fundador de Foresenics

Un delito silencioso que perjudica a una empresa desde adentro.

En la antesala del fraude informático está la seguridad informática

El fraude interno es un delito que generalmente no incluye violencia física y cuyo propósito principal es obtener ganancias financieras. Pueden cometerlo gerentes, directores, jefes, es decir personal calificado o jerarquizado de una empresa. Pero también pueden ser trabajadores en el campo de extracción y, desde ya, cualquier empresa puede ser víctima.

Como el 90% de los documentos comerciales son electrónicos, los fraudes internos se preparan y realizan a través de herramientas digitales. Sería extraño investigar y descubrir un fraude que no se cometa usando correos electrónicos, servidores, programas, imágenes electrónicas, cámaras digitales, ordenadores, teléfonos celulares o redes sociales.

El universo digital, entonces, es el medio natural en el que se preparan y perpetran los fraudes. Y es un medio vulnerable también en la industria del petróleo. En efecto, según el informe "The State of Cyber Security in the Oil & Gas Industry: United States"[1], presentado por el Instituto Ponemon de los Estados Unidos, entre 2016 y 2017, alrededor del 70% de las empresas de gas y petróleo en los Estados Unidos fueron hackeadas o sufrieron algún tipo de ataque cibernético, y el riesgo de sufrir ese tipo de vulnerabilidad sobre todo en la parte operacional, está presente en, al menos, 65 de las empresas de esa industria. El informe establece que solo en los Estados Unidos el 35% de los encuestados calificó la disponibilidad cibernética de su organización de tecnología operacional (OT) como alta.

Fraude interno, de flagelo a epidemia

El fraude interno es un delito temido por las empresas y no hay informe anual de especialistas que así no lo reflejen[2]. La mayor parte de las investigaciones internas realizadas durante 2016/2017 en el ámbito interno de firmas argentinas tuvieron por finalidad detectar fraudes y obtener la prueba electrónica necesaria para fundar las acciones legales pertinentes[3].

Un riesgo democrático

Los mayores fraudes involucran celulares, servidores laptops y PCs. Las áreas de sistemas y de compras nunca parecen estar suficientemente bien protegidas. ¿Y las áreas de administración y de recursos humanos? Se me ocurre, por la experiencia en investigaciones internas, que no hay área que se salve. Antes las empresas miraban afuera para prevenir fraudes, ahora miran hacia adentro.

La reacción: tarde, casi siempre

No existe, en general, una cultura de prevención en este punto. Prevenir es gastar y eso es anatema en algunos casos, aunque las consecuencias del fraude sean infinitamente más costosas[4]. La actitud de la alta gerencia frente al fraude suele ser reactiva. O al menos lo era: en la Argentina la responsabilidad civil y penal de directorio se ha extendido notablemente en los últimos tiempos. Pero lo cierto es que más de la mitad de los fraudes en las empresas son descubiertos por coincidencia, ya sea por información obtenida por medios externos, accidentes, o cambios en la administración. Una vez que la presunción de un fraude gana fuerza, el cliente se acerca al especialista en busca de pruebas. Entonces, investigar la actividad digital del sospechoso es esencial.

Un límite inicial y como sortearlo

Al comenzar la investigación, que bien puede ser anterior a la comisión efectiva, en la etapa de "preparativos", es necesario conocer los límites y facultades legales de la empresa para acceder a las fuentes. Hay que determinar si la empresa está facultada para monitorear y controlar el contenido de la información que se encuentra alojada en ordenadores, GPS, laptops, servidores, celulares, tarjetas de acceso a la planta, redes sociales del empleado o la misma empresa.

¿Cuáles son los requisitos, entonces, para poder investigar, en este sentido, al empleado?

- El empleado debe haber consentido expresa y reiteradamente la facultad del empleador de monitorear su actividad, encuadrada en el control de los elementos de trabajo de su propiedad, puestos al servicio del empleado conforme los argumentos de los artículos 70, 71 y 72 de la Ley de Contrato de Trabajo.
- El documento en el que el empleado debe hacer constar su consentimiento, al tiempo mismo de su incorporación, debe aclarar que el empleador podrá realizar las investigaciones y los controles que resulten necesarios, tanto de los equipos como de las herramientas que le facilitada al empleado. Existiendo este documento, que debe ser periódicamente notificado al empleado, en el que este consiente el monitoreo de las herramientas digitales que son propiedad del empleador, la jurisprudencia nacional, desde hace más de once años (Cfr. P.R.F. c/ Ceteco Argentina SA s/ despido», CNTrab, Sala I, 29/04/2005) ve con buenos ojos el ejercicio de esta facultad.
- El dispositivo, PC, laptop, tablet, celular donde se realice este control, debe ser propiedad de la empresa. Se incluyen los sistemas de telefonía fija, móvil, telefonía IP, correo electrónico, sistemas de mensajería instantánea o cualquier otro medio electrónico que pone a disposición de su personal para comunicarse en el ámbito laboral. De hecho, es la naturaleza de dichos medios como herramientas de producción la que legitima el control y el monitoreo de su uso.

Cómo proceder luego del acceso a la información

Cuando la empresa ha accedido a la información, hay que seguir un protocolo que le de validez legal de "prueba" a los hallazgos, que bien pueden terminar en manos de un juez que evaluará su integridad forense. En este punto, les propongo seguir un texto con preguntas y respuestas. Es un método práctico donde el lector se puede identificar con quién pregunta:

¿Hay un procedimiento establecido?

Depende de la empresa. En mi experiencia, las firmas internacionales tienden a seguir los protocolos de sus casas

matrices. No es infrecuente que cuando detecten un hallazgo, se comuniquen con ellas en busca de instrucciones. Ello puede ser contraproducente, porque la ley argentina es particular en el tratamiento de la prueba digital. Y su falta de seguimiento da lugar a nulidades.

¿El tema se resuelve internamente?

Existe una fuerte tendencia a solucionar estos temas discretamente. A lo sumo, en el ámbito de una conciliación o mediación anterior a la etapa judicial.

¿Cómo lo detectan?

Hay evidencias concretas: cambio de estilo de vida, viajes al exterior, membresías a clubes exclusivos, cambio de colegios, mudanzas, compra de autos de alta gama y propiedades o segundas propiedades.

¿Cómo lo investigan?

Siempre hay un rastro digital. Hay que identificarlo y obtener de inmediato una copia forense (que no es un backup) Luego, analizar la evidencia, es decir todo lo que está en el disco rígido o la memoria móvil para buscar y comprobar el fraude y la cadena de responsabilidades.

¿Qué es la cadena de custodia?

Los documentos digitales tienen poder de convicción si son integros. Para eso hay que evitar su contaminación desde que se extraen hasta que se presentan en juicio. La tarea de protección de la prueba digital consiste en establecer una "cadena de custodia". La cadena de custodia debe decir dónde y cómo se ha obtenido el documento, que se ha hecho con él (y cuándo), quién ha tenido acceso a ese procedimeinto (punto esencial a la hora de defender su pureza), dónde se encuentra el documento en todo momento y quién lo tiene y, en caso de eliminación, cómo, cuándo, quién y por qué lo ha eliminado.

El estudio de la prueba digital no se practica sobre el original del documento –disco rígido, por ejemplo– sino sobre una copia. La ventaja es que el original quedará a salvo de riesgos físicos. Respecto de estas copias, deberá crearse una cadena de custodia independiente que haga referencia a su procedencia. Aquí es conveniente que alguien testifique qué se copia y cómo. En realidad, no es solamente "copiar" lo que debe hacerse, es copiar bit por bit y generar una huella digital de modo que no haya confusiones o "agujeros negros". Un soporte como un Pen o un CD complementará, si es necesario, una presentación judicial.

¿Hay jurisprudencia en la materia?

Sí, pero no hay principios excluyentes que rigen estos casos. Hay que poner atención a las decisiones de los tribunales atinentes a límites a la privacidad y a la forma en que se tomó la evidencia.

Las entrevistas

En un primer momento, la empresa que es víctima puede considerar la posibilidad de entrevistar al sospechoso. ¿Es efectivo? No sabría decirlo. Las entrevistas pueden dar una noción, pero la verdad es que un abogado hábil puede cuestionar la validez de los resultados una vez que el conflicto escale. Fuera del ámbito de una audiencia judicial, tomada con las garantías constitucionales de defensa en juicio, no es mucho lo que puede lograrse preguntando a los sospechosos si fueron ellos.

Conclusión: solo buenas prácticas

Este trabajo no constituye una opinión legal ni un consejo legal. Es más bien, una descripción de buenas práctica a la hora de investigar un fraude interno. Quizás la mejor práctica es la pregunta ¿por qué no puede ocurrirle a mi empresa?

1 "Industria petrolera sufre de ataques cibernéticos: SIEMENS", ver: http://ganar-ganar.mx/industria-petrolera-sufre-de-ataques-ciberneticos-siemens
2 "The Top Fraud of 2017". Federal Trade Commission, Consumer Information, March 1st, 2018.
3 Fuente: Foresenics Argentina, investigaciones comprendidas en el período Junio 2016-Junio 2017.
4 "FRAUD PREVENTION STRATEGY SERIES - PROACTIVE MEASURES", by Stephen Reed, CPA, PSA, CGMA