EL COMPLIANCE Y EL RIESGO DE FRAUDE II

NOTI 272 - Febrero de 2018

Una vez se reciba una denuncia por fraudes y eventos irregulares, la primera actividad será la de tratar de determinar el grado de credibilidad de la información recibida, ya que puede tratarse de un dato falso, o uno tendiente a desviar una investigación en curso; o simplemente un intento por perjudicar a alguien acusándolo injustamente.

Fuente: http: http://www.legalisconsultores.es/2016/07/corporate-compiance-cumplimiento-normativo-en-las-empresas/

- **Escenario #2:** Cuando la empresa es el objetivo: en este escenario todavía no se ha producido el evento, pero la empresa recibe información confiable de que se encuentra en la mira de los defraudadores.

Más del 44% de los fraudes se descubre por denuncias recibidas en los distintos canales que las empresas ponen a disposición de las personas interesadas en denunciar. Las denominadas "LÍNEAS ÉTICAS" son el mejor vehículo para recibir este tipo de información, ya que los denunciantes las prefieren por sobre canales tradicionales como los buzones internos, las páginas web o los correos electrónicos corporativos.

Una vez recibida la denuncia, esta deberá ser dirigida al equipo de análisis correspondiente. La primera actividad será la de tratar de determinar el grado de credibilidad de la información recibida, ya que puede tratarse de un dato falso, o uno tendiente a desviar una investigación en curso; o simplemente un intento por perjudicar a alguien acusándolo injustamente. Lo importante es que cada denuncia sea recibida, analizada y tratada en consecuencia. No queremos lamentar el no haber actuado a tiempo por desestimar una denuncia que al comienzo parecía fantasiosa.

Más del 44% de los fraudes se descubre por denuncias recibidas en los distintos canales que las empresas ponen a disposición de las personas interesadas en denunciar.

Fuente: http://www.aeaecompliance.com/

Si se considera creíble, deberá entonces comenzar de inmediato el proceso de respuesta que sea más adecuado para la situación que se plantea. Veamos un ejemplo. En el correo corporativo de una empresa se recibió una denuncia anónima, según la cual la organización se encontraba en la mira de un grupo de hackers, quienes estaban preparando un plan para violar la seguridad electrónica e implantar un software malicioso que les permitiese encriptar la información sensible de la compañía y luego pedir una cuantiosa suma de dinero en Bitcoins para des encriptarla. Indicaba el anónimo que al menos un empleado del área de TI de la compañía podría estar involucrado con los delincuentes externos.

Al analizar la información recibida, la empresa decidió actuar de la siguiente manera:

1) Establecer cómo puede materializare la amenaza detectada, para proceder a intervenir las situaciones, procesos o sistemas que podrían vulnerarse. Se determinó que sí podrían ser víctimas de un esquema como el sugerido;

2) Involucrar a las áreas que debían participar en la ejecución de las tareas tendientes a evitar el daño. Se debería convocar a las áreas de Tecnología de la Información, Seguridad física, Archivo, Talento humano, Jurídica y Financiera, bajo la coordinación del área de Gestión de Riesgos. Teniendo en cuenta la denuncia sobre un posible empleado de TI involucrado en el caso, se decidió solo hablar con el director del área y autorizarlo para contratar expertos de afuera para su trabajo;

3) Se decidió en el instante adquirir un servidor separado de los que se tenían trabajando y hacer copias cada 6 horas de la información sensible, la cual se mantendría fuera de la red y con las restricciones de acceso necesarias para evitar que este servidor resultase infectado;

4) Contratar un experto para realizar pruebas de intrusión, (Ethical Hacking), con el propósito de identificar vulnerabilidades y corregirlas. Especial énfasis se debería hacer en el uso de redes sociales por parte de los empleados y la posibilidad de que estos instalaran programas no autorizados en los sistemas de la empresa;

5) Revisar los contratos de trabajo de los empleados, para insertar cláusulas que expresamente prohíban el uso de los recursos y sistemas de la empresa para propósitos privados; esto es, se prohibía almacenar o transmitir información no relacionada con el objeto social;

Fuente: http://garciamontoliu.com/compliance/

Carrera 43B N° 16-41
Medellín, Colombia
+57 4 266 33 42
asr@asr.com.co
http://www.asr.com.co/

6) Comenzar una labor de investigación discreta de los empleados del área de Sistemas, con el fin de determinar si alguno de ellos estaba efectivamente involucrado en el intento criminal contra la empresa.
7)
En este caso el ataque efectivamente ocurrió a los dos meses de haber recibido el aviso, pero la preparación de la empresa logró limitar el daño, ya que solo resultó comprometida información de 6 horas, la cual pudo ser reconstruida de manera documental. La investigación posterior permitió identificar no solo al empleado interno cómplice de este crimen, también ubicar la fuente externa del ataque. Las lecciones aprendidas sirvieron para reforzar los controles y aumentar la confianza del equipo gerencial en su capacidad para afrontar amenazas de este tipo.

Continuaremos.

asr@asr.com.co