Reflexiones sobre el fraude personal y corporativo

El nuevo mundo interconectado genera tension en términos de seguridad y los controles terminan siendo los más simples, guiados por el sentido común.

Juan Carlos Reyes M.

El vocablo latino *fraus* es aquel de donde deriva la palabra fraude, y su significado más simple es el de la "acción que resulta contraria a la verdad y a la rectitud".

Partiendo de esta sencilla pero completísima definición, se ha desarrollado una impresionante cantidad de prefijos para indicar de qué manera se puede cometer cada tipo de fraude, hasta llegar a uno de los más recientes que es el anglicismo *ciber*, generalmente utilizado para referirse a lo que comprende el mundo digital de los sistemas de información, incluso el internet.

Podríamos señalar que es de esta forma como etimológicamente se configura el ciberfraude. Pero, nada más alejado de la realidad creer que el *ciberfraude* es sólo una formación de palabras, cuando nuestra sociedad actual es cada vez más *ciber* dependiente. Al final, vivimos en un mundo

que mantiene las más viejas costumbres (como el *fraus*), pero que tiene todas las oportunidades de las nuevas tecnologías (el *ciber*).

Una de las aristas más apasionantes en torno a este tema es darse cuenta de que la única diferencia entre hace 100 años y ahora, es sólo el medio por el cual se produce. Donald Cressey en su libro "The Theft of Nation" establece una de las teorías más comúnmente aceptadas hoy, sobre por qué la gente comete fraude, llamada "el triángulo de cressey" que se apuntala en tres conceptos básicos:

Motivación: ¿qué es lo que motiva al defraudador a cometer el ilícito? Tal vez tiene problemas económicos, alguna presión financiera, gasta en forma excesiva, mantiene un estilo de vida en contravía con sus ingresos o está forzado a conseguir dinero (para pagar alguna extorsión, por ejemplo).

Oportunidad: ¿el defraudador, además de la motivación, tiene la oportunidad de cometer el fraude? ¿Es alguien que tiene acceso al dinero, a los bienes o que tiene la autonomía para negociar con ellos y obtener un beneficio personal? ¿Es el administrador de un sistema transaccional, con los privilegios para eliminar registros o abrir la puerta a los datos?

Mucho hemos oído hablar en diferentes escenarios acerca de la motivación y la oportunidad y resulta lógico entender que si las dos existen, el fraude está hecho. Pero, la verdad es que no es así.

Lo más impactante de la teoría de Cressey, aquello que la aleja de la lógica es el tercer elemento que conforma el triángulo, porque es tan humano e inherente al ser, que incluso nos brinda una dimensión adicional, sin la cual aun cuando existiera la oportunidad y la motivación, el humano no cometería un fraude: la racionalización.

Racionalización: cuando el defraudador tiene la motivación y la oportunidad, debe vencer una última barrera, que es él mismo; debe auto convencerse de que el fraude que está a punto de cometer no es ilegal y tiene que justificarlo, no para sus jefes o sus compañeros sino para sí mismo. Esto es lo verdaderamente excitante de la teoría de Cressey. El defraudador debe pensar que se MERECE lo que hace, culpando al sistema, a la sociedad o a su entorno. Frases como "he trabajado mucho y no lo reconocen" o "nadie se dará cuenta" o "lograré compensarlo antes de que se enteren" están a la orden del día para satisfacer la necesidad de racionalización del individuo, como parte de la argumentación que usará si alguien se refiere al tema.

Bien sea que el defraudador tenga acceso al dinero físico o al sistema de información, esta conducta siempre es repetitiva, sea para fraudes tradicionales o informáticos. Al final no hay juez más duro que uno mismo.

La evolución de las tendencias de fraude presenta múltiples oportunidades a partir del desconocimiento y de la ingenuidad de las personas cuando de elementos informáticos se trata. Numerosos estudios demuestran que las poblaciones más afectadas por el fraude digital son las personas mayores, los ancianos, sobre todo, en cuanto al fraude financiero; y menores,

en lo relacionado con el acoso en línea. Estos resultados tienen sentido si tenemos en cuenta que la población que ha crecido conociendo internet y las nuevas tecnologías es más escéptica frente a lo que encuentran en línea, que aquellos que no están familiarizados con las mismas.

Entrando en materia, desde nuestro observatorio de fraude hemos podido evidenciar cómo se han vuelto más sofisticados los ataques hacia la población en general. Hace algunos años era muy evidente que los correos electrónicos de phishing buscaban su objetivo lo más directamente posible, al solicitar abiertamente la contraseña de acceso, mientras que hoy en día estos correos ni siquiera parecen estar interesados en ella, sino más bien en información común como datos de identificación o georeferenciación. Incluso es más probable que busquen instalar alguna clase de malware en el computador o en el teléfono, con miras a monitorear las actividades y/o crear redes zombis que atacan al unísono como botnets, una de las armas cibernéticas más letales debido a su estructura colaborativa.

Por supuesto el gran reto lo tiene el usuario común y corriente, pues cada vez le es más difícil identificar lo que puede ser *malware* o no; las aplicaciones que instala en su teléfono por ejemplo pueden ser las más inocentes y no saber cuáles son sus verdaderas intenciones: hemos encontrado aplicaciones para encender la linterna del teléfono que al instalarse piden permiso para acceder a la agenda de contactos del teléfono, lo cual es absolutamente innecesario. A mismo tiempo que el usuario se expone a la victimización, se convierte en un objetivo más apetecido por los ciberdelincuentes, pues al poder trazar al detalle sus actividades y perfilar sus rutinas es posible determinar su perfil económico, social, profesional y digital.

Los fraudes dirigidos a los usuarios de tecnología tienen como componente principal aprovechar la confianza creciente que experimentamos en las tecnologías de información, pues hoy toda nuestra vida está entre dos aparatos que son el computador y el teléfono. Nuestra música, nuestros intereses, nuestras relaciones, nuestra información, nuestras fotos, nuestra ubicación, y en algunos casos, hasta nuestro dinero pueden estar en esos dos aparatos, lo que los convierte en objetivos de alto valor para escalar hacia fraudes más globales, como, por ejemplo las corporaciones donde trabajamos. Y es ahí donde toma sentido el concepto del "valor digital" de una persona: qué hace dentro de su compañía, a qué tipo de información o activos tiene acceso, sumado a saber si tiene la necesidad y la motivación para cometer un fraude.

Las redes sociales juegan un papel clave hoy en día en la preparación de fraudes, con la entrada del concepto de OSINT (Inteligencia de fuente abierta) que se basa en la perfilación de las personas, a partir de su actividad en internet, principalmente en sitios sociales donde publican detalles de su vida diaria. En internet existen herramientas y personas que "cosechan" toda esa información para crear datos de tendencias en cuanto a intereses, información demográfica, geográfica y muchas otras que, al final, facilitan desde el envío de publicidad

altamente dirigida (*marketing*) hasta la sofisticación del *phishing* con datos bastante específicos que podrían llegar a engañarlo.

Por otro lado, no se puede separar el fraude personal del fraude corporativo, toda vez que cuenta con los mismos actores, sólo que en situaciones diferentes en donde la persona puede pasar de ser víctima a perpetrador, o simplemente terminar siendo un soldado en favor de organizaciones criminales complejas.

En razón del trabajo que desarrollamos en AntiFraude® hemos conocido de primera mano muchas situaciones de fraude que han sido facilitadas por la tecnología, bien sea porque ésta ha sido modificada de manera maliciosa por alguien que tenía el acceso a ella o simplemente porque funcionarios internos han aprovechado la oportunidad cuando hay problemas tecnológicos. En cualquier caso, los fraudes corporativos se siguen encuadrando en las tres grandes categorías sugeridas por ACFE, en su reporte a las naciones: Corrupción, apropiación indebida de activos y fraude en estados financieros, todos éstos facilitados por las cada vez más numerosas herramientas informáticas de que disponemos.

Si bien el fraude como conducta dentro de una organización puede ser muy difícil de acabar completamente, si es posible disminuirlo a través de los controles apropiados. Una efectiva estrategia de control involucra por una parte, las acciones preventivas que permitan disuadir el fraude como, por ejemplo, la ubicación de elementos de monitoreo (audio, video, informático) dentro del marco de la ley y de los derechos fundamentales, la promulgación de políticas de prevención de fraude y las técnicas para evitar la colusión.

El análisis adecuado de la cultura organizacional, la identificación de competencias de las personas clave en la organización y una adecuada gestión de cambio totalmente alineada con las competencias existentes y el estilo de cultura organizacional propio, son factores determinantes para disuadir las posibilidades de fraude e identificar de forma temprana dónde puede haber vulnerabilidades de carácter humano.

Por otro lado, el ambiente de control debe proporcionar los mecanismos para identificar los fraudes, bien sea mediante el uso de líneas o la asignación de recompensas por información o tal vez mediante las auditorías y otros mecanismos de investigación, que permitan establecer cómo se presenta una conducta fraudulenta.

Finalmente, se deben tener adecuados mecanismos de reacción, para que cuando se identifique una situación sea posible acceder rápidamente a la causa raíz de la misma para eliminarla y garantizar que no vuelva a suceder.

Hoy en día, la evolución tecnológica ha llevado inclusive a contar con herramientas adicionales para transferir el riesgo de fraude, como las pólizas de seguro, en las cuales ya hay aproximaciones muy detalladas acerca de coberturas para riesgo cibernético. Así mismo, la tercerización de procesos operativos toma un papel protagónico en la transferencia del riesgo, bajo la premisa de que puede ser más expedi-

to tomar acciones legales contra un proveedor que ha cometido fraude, que contra un empleado.

En conclusión, no podemos separar el fraude que afecta a las personas comunes y corrientes, del fraude que afecta a las organizaciones. Las herramientas tecnológicas para ejecutar diversos esquemas de fraude complejos están a la orden del día y la realidad es que se pueden conseguir a muy bajo costo en la red cuando se sabe a dónde buscar.

Por otro lado, todos los días, tanto a título personal como corporativo, producimos demasiada información hacia la red y siempre hay alguien que está tomándola para perfilar las actividades y conocer a los potenciales objetivos. Sin embargo, en medio de toda la preocupación que puede generar el nuevo mundo interconectado en el que vivimos, las soluciones siguen siendo las más simples, y están en el sentido común.

Juan Carlos Reyes Muñoz. *Director de la firma Grupo Schart Latinoamérica especializada en seguridad de la información aplicada al fraude, mediante la marca AntiFraude®. Miembro de la Asociación de Investigadores de Crímenes de Alta Tecnología (*www.htcia.org*), de ACFE (*www.acfe.com*), auditor líder de ISO 27001 y delegado para el comité JTC1/SC27 de ISO en representación de INLAC, con una experiencia de más de 15 años en seguridad de la información en diferentes instituciones financieras, de seguros, de servicios y gubernamentales alrededor de América Latina.*