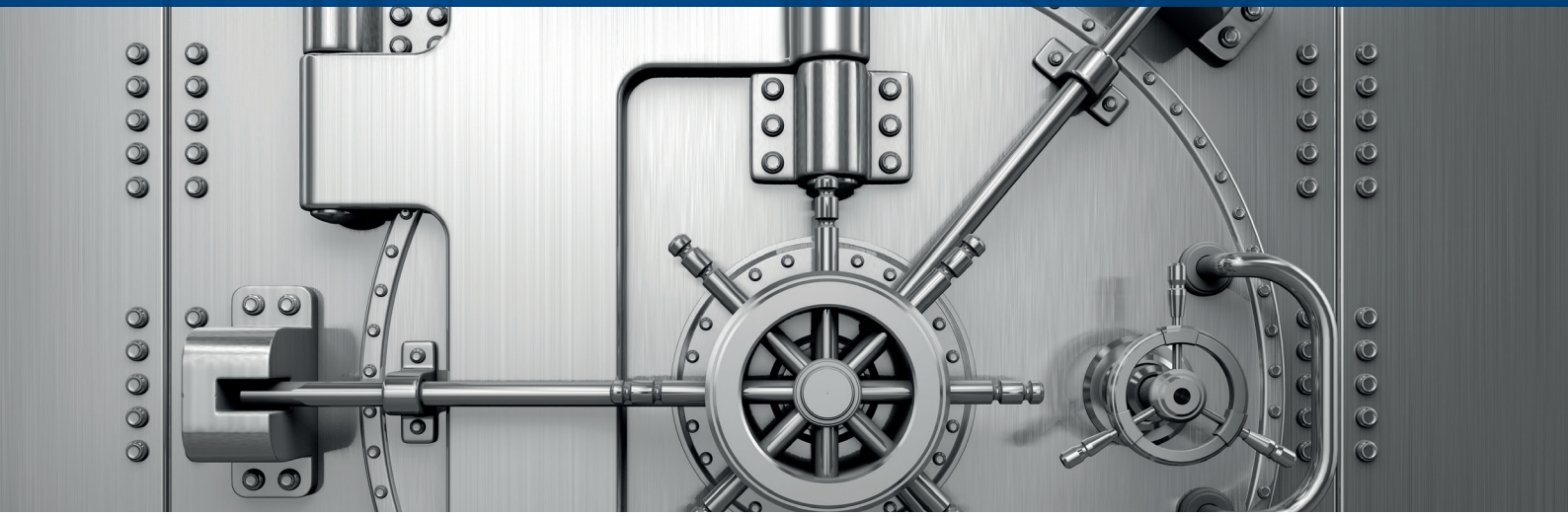


Dañando más que el Resultado Final: Un panorama acerca del fraude y de la Seguridad Cibernética.

Todos hemos visto las cifras referentes al costo del fraude y de los ciberataques a las empresas y la economía con algunas estimaciones que ubican el costo global en los USD 445 mil millones*. Sin embargo, menos sensacionales pero mucho más perjudiciales que las implicancias financieras son el daño a la reputación y el impacto en el negocio que surgen como consecuencia de los ataques exitosos.

Protegerse de las amenazas y los ataques que representan el fraude y la seguridad cibernética, hoy en día, es una preocupación creciente para las empresas. Para muchos, se ha vuelto imperativo salvaguardar sus organizaciones de tales peligros, especialmente si consideramos que las amenazas y los ataques siguen sin ser abatidos así como también los métodos de los estafadores y los atacantes, evolucionan y se modifican para lograr sus fines.

Existe información disponible que indica que las instancias de fraude y de los ataques a la seguridad cibernética están aumentando no solo en frecuencia, sino también en severidad e impacto. Las compañías que fallan en asegurarse que sus empleados estén bien capacitados para reconocer y actuar en contra de esto, utilizando procesos, procedimientos y protocolos de seguridad adecuados, no solo corren un mayor riesgo de pérdidas financieras, incluyendo pérdida de activos, sino también un mayor riesgo de daño reputacional e interrupción del negocio, incluyendo publicidad negativa.

¿Cómo ha cambiado el escenario del fraude?

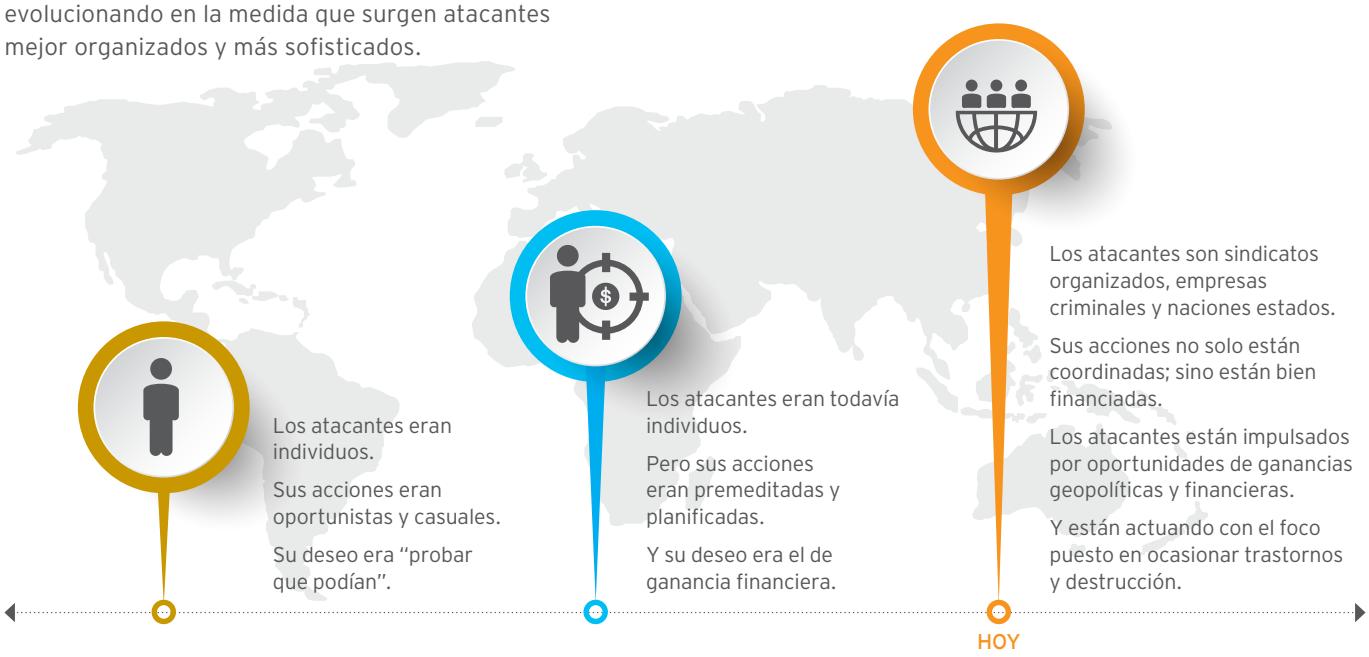
El fraude y las amenazas a la seguridad cibernética continúan evolucionando a medida que surgen atacantes mejor organizados y más sofisticados.

Tal como está ilustrado en el diagrama 1, en los últimos años los estafadores y los atacantes cibernéticos se han vuelto más sofisticados. Ha habido un notable giro en el perfil de aquellos individuos detrás de los ataques.

*De Pérdidas Netas de McAfee: Estimando el Costo Global del Crimen Cibernético, la descarga más reciente de www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf del 4 de abril de 2016.

Diagrama 1. – Del Pasado al Presente: El Cambio Radical en las Amenazas a la Seguridad de la Información

El escenario de la amenaza cibernética continúa evolucionando en la medida que surgen atacantes mejor organizados y más sofisticados.



En el pasado, los atacantes eran básicamente individuos operando de manera oportunista, casual o ad hoc, mayormente impulsados por el deseo de probar que podían llevar a cabo un ataque de fraude de manera exitosa.

Actuando solos o en conjunto para cometer fraude interno o externo, los estafadores, cada vez más, llevan a cabo actos que se enfocan en ocasionar trastornos y destrucción.

Hoy, los atacantes son sindicatos y empresas criminales altamente organizadas que son manejadas de manera similar a las compañías. Estas empresas criminales están normalmente bien organizadas y, más importante, bien financiadas. Están motivados básicamente por las ganancias financieras pero en algunos casos por los beneficios geopolíticos. Estos estafadores están cada vez más enfocados en ocasionar trastornos y destrucción. Existe también el riesgo de fraude interno y, de la misma manera, el fraude interno puede ser realizado por individuos oportunistas o por un empleado que opera en conjunto con un grupo del crimen organizado.

El Diagrama 2 muestra la naturaleza cambiante de los múltiples aspectos del fraude o ataque a la seguridad cibernética. Notablemente, los ataques tienen objetivos cada vez más específicos con atacantes que llevan a cabo una extensa investigación y planificación previa al intento de ataque. Los intentos de ataque también cambiaron de patrones de ataques oportunistas realizados por única vez hacia ataques dirigidos, planificados y continuos. Los atacantes continuarán sus intentos hacia un objetivo si existe la posibilidad de éxito.

Los métodos de ataques también se encuentran en evolución constante y se adaptan para superar las defensas que generan las organizaciones. No es sorprendente que haya habido un incremento en el uso de tecnología por parte de los estafadores. Los métodos de ataque tienden a tomar como objeto las debilidades en la tecnología y en la naturaleza humana y en algunas instancias, en ambos. Es por esta razón que es muy importante revisar frecuentemente los procedimientos y procesos internos y asegurar que todos los empleados estén exhaustivamente capacitados y conscientes de sus responsabilidades ante un intento de ataque.

¿Cuál es el perfil de un estafador?

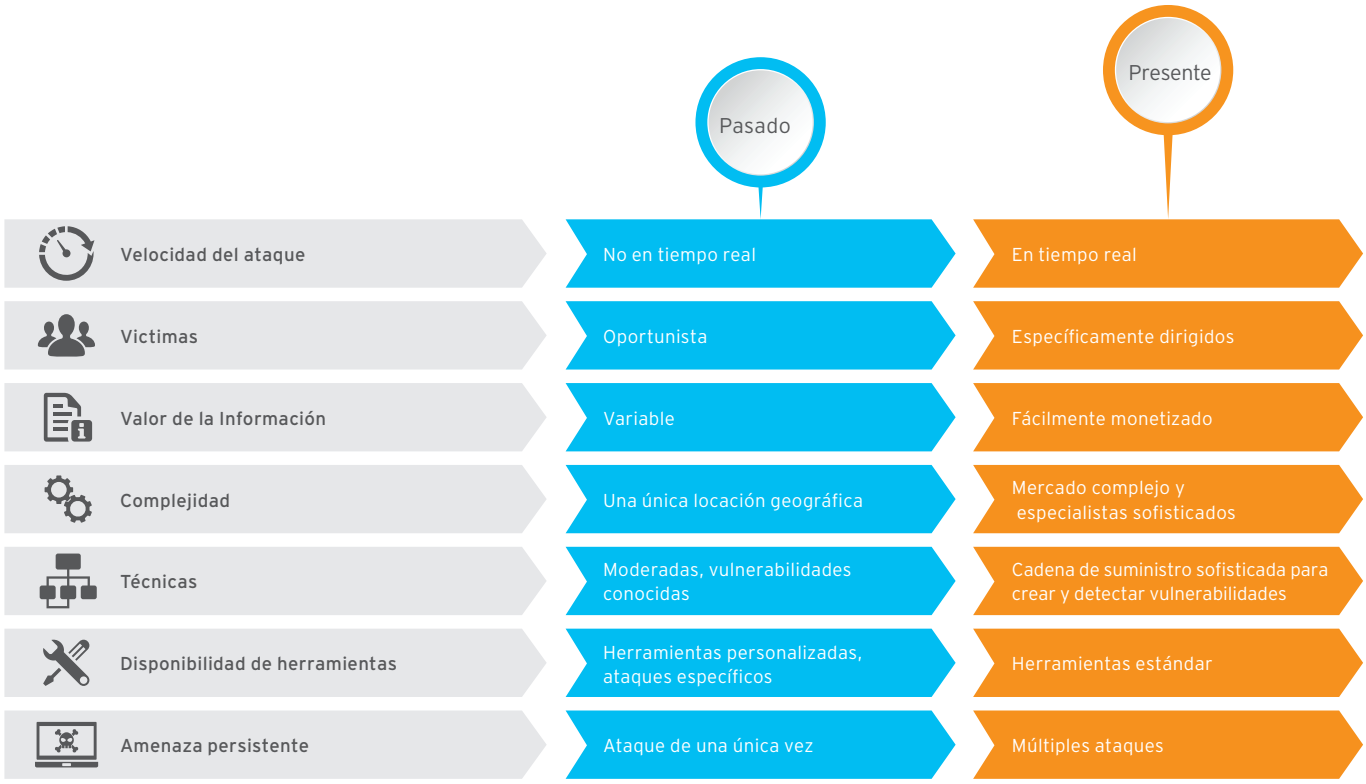
KPMG ha desarrollado el perfil de un estafador interno promedio sobre la base de un estudio de 596 casos de crímenes realizados por empleados administrativos entre los años 2011 y 2013, con algunas estadísticas reveladoras.

Su objetivo son sus empleadores

El típico estafador es masculino y tiene entre 36 y 55 años, y tiende a cometer fraude en contra de su propio empleador.

- 61% de los estafadores son empleados por la compañía que atacan.
- 41% están empleados por un periodo mayor a los 6 años.

Diagrama 2. Amenazas en Evolución: Una ilustración de los desafíos de Seguridad de la Información.



Trabaja en Connivencia

Tiende a trabajar en un puesto de finanzas o relacionado a ellas, incluyendo el departamento de operaciones, o tienen puestos gerenciales. Como tales, generalmente han sido empleados por su compañía por más de 6 años. Durante este tiempo, en el 72% de los casos han realizado fraudes durante 1 a 5 años, donde el 70% de las veces, trabaja en connivencia, causando daños por decenas de miles, cientos de miles y aun millones de dólares.

- 18% son valuados entre $50.000 y $200.000.
- 43% exceden los $500.000, 16% de los cuales exceden los $5.000.000.

También trabaja por su cuenta

Cuando este estafador promedio trabaja solo, una gran mayoría de los fraudes que comete ocurren entre 1 y 5 años, también causando un daño económico significativo.

- 21% son valuados entre $50.000 y $200.000.
- 32% exceden los $500.000, 9% de los cuales exceden los $5.000.000.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions

1462069 08/16