Boletín Informativo / Septiembre 2017

UPCLC/FT

Tema: DEFENDERSE DE LOS ESTAFADORES: SEIS PASOS PARA LA LUCHA CONTRA LA DELINCUENCIA FINANCIERA EN LA BANCA DE HOY.

En la industria de servicios financieros, tecnología de punta es generalmente visto como un facilitador del crecimiento del negocio, así como una experiencia de consumo mejorada. Por ejemplo, libros de contabilidad blockchain tienen el potencial de acelerar significativamente los pagos internacionales y también revolucionar la forma de registros de clientes se almacenan. Sin embargo, el rápido avance en las técnicas de delitos informáticos significa que la fusión de los servicios financieros con la tecnología es, en realidad, a veces, poniendo en peligro los activos.

Los ciberdelincuentes están constantemente tratando de orientar nuestra riqueza y nuestras identidades, y las amenazas están cobrando impulso. De hecho, se espera que los delitos financieros, costaran a las empresas más de $ 2 trillón a nivel mundial para el año 2019. Esta cifra es una combinación de lavado de dinero, delitos informáticos, el fraude y la evasión de impuestos. Como resultado de factores tales como la globalización, la proliferación de canales bancarios, el aumento de los volúmenes de transacciones y los avances en la tecnología, las empresas financieras de todos los tamaños son cada vez más vulnerables a medida que luchan para mantenerse al día con las técnicas sofisticadas que se asocian con el hacker de hoy.

Al mismo tiempo, las instituciones financieras se enfrentan a constante evolución requisitos normativos, incluyendo el cumplimiento AML actualizado (Anti-Lavado de Dinero). De hecho, una serie de bancos de alto perfil se han enfrentado a las sanciones y las críticas sobre los controles contra el lavado de dinero, incluyendo Deutsche Bank y Swiss Bank BSI . Con fuertes sanciones en el lugar para los no adaptarse lo suficientemente rápido como defensas, un precedente se está estableciendo una mayor transparencia, la responsabilidad y el cumplimiento. A pesar de los bancos de hacer grandes inversiones en medidas de seguridad y cumplimiento, un enfoque fragmentado de los delitos financieros puede limitar su éxito en la prevención de la misma. Sin lugar a dudas, los bancos tienen que adaptarse continuamente y mejorar sus políticas y enfoque para luchar contra la delincuencia informática para proteger los activos de datos y optimizar los ingresos. Aquí se recomienda seis pasos para hacer frente a estos problemas:

1) Adaptar el proceso de gestión de riesgos

Crucial para el desarrollo de controles de seguridad adecuadas es la adquisición de conocimientos acerca de los posibles riesgos y cómo podrían afectar al negocio. La realización de la evaluación exhaustiva de los riesgos adecuada y la cartografía de los resultados respecto a las políticas internas, procedimientos y controles puede permitir a los bancos para evaluar su capacidad para mitigar los riesgos y adaptarse en consecuencia. Teniendo en cuenta el tamaño, canales, zonas geográficas de una organización y tipos de clientes, y re-evaluación de la estrategia regularmente como estos factores cambian se asegurará de que los planes de gestión de riesgos de una empresa siguen siendo pertinentes.

2) Dirección silos internos

El amplio espectro de delitos financieros, desde el lavado de dinero a los ataques cibernéticos, significa que los bancos son a menudo la tentación de fusionar las diversas funciones encargadas de la prevención del delito. Sin embargo, demasiado de esta puede aumentar la vulnerabilidad; de hecho, un mejor enfoque es mejorar la comunicación interna y la coordinación entre las funciones. Por ejemplo, la ciberdelincuencia y AML disciplinas se enfrentan a retos similares y con frecuencia se superponen en términos de procesos, sistemas y requisitos de datos. Por lo tanto, como estos equipos con funciones similares están en una gran posición para intercambiar puntos de vista.

3) Superar desafíos de datos

Clave para la gestión de riesgos es la adquisición de alta calidad y de datos de toda la organización, algo que no siempre es fácil para los grandes bancos que se han acumulado datos de múltiples sistemas como resultado de las fusiones y adquisiciones. La normalización de grandes volúmenes de datos de los clientes y de transacciones puede mejorar significativamente la calidad general de los datos y proporcionar la precisión necesaria para apoyar el monitoreo en tiempo real y la toma de decisiones basada en datos. La clave para lograr esto es asegurarse de que los empleados se adhieran a las normas internas al introducir los datos.

4) La aplicación de la analítica avanzada

Acumular los datos relevantes es importante, pero utilizando de manera eficaz es otro factor por completo. El uso de análisis y visualización de datos es ahora esencial para combatir los delincuentes cibernéticos, y comprender los patrones de amenaza. Mientras que los bancos ya se están recogiendo datos de los clientes para satisfacer Conozca a su Cliente (KYC) regulaciones, análisis adicional de los datos de punto de venta, medios de comunicación social, las bases de datos de clientes y de fuentes externas como proveedores de datos permite a las empresas de servicios financieros para mejorar la velocidad de detección de fraude y predicción. Sólo por investigar más profundamente en estos datos son instituciones financieras capaces de comprender mejor los riesgos planteados por los clientes, transacciones y otras entidades y descubrir amenazas complejas con el potencial de impactar varias líneas de negocio.

5) Dar ejemplo

Para cruzada contra la delincuencia financiera, los bancos deben asegurarse de que los empleados más antiguos dan el tono mediante el establecimiento de estándares de rendición de cuentas, controles y políticas. La administración también debe promover la transparencia, trabajando estrechamente con los reguladores y dar incentivos para el cumplimiento. Un aspecto importante de esta es la formación de los empleados sobre los últimos desarrollos normativos y sensibilización interna de amenazas emergentes, tales como los riesgos asociados con las monedas virtuales y las nuevas tecnologías.

6) Colaborar con las iniciativas de toda la industria

Algunas empresas han desarrollado sus propias herramientas propias para desarrollar soluciones sostenibles de prevención del delito y escalables, un-guiada por las mejores prácticas en general. Aunque teniendo en cuenta los estándares de la industria es clave, las instituciones financieras deberían colaborar con la industria más amplia de reevaluar sus estrategias de forma regular y mantenerse al día con las políticas cambiantes. Restante estancada puede dar lugar a la duplicación de esfuerzos en toda la industria y los costos adicionales de cumplimiento. Los bancos que toman un enfoque unificado pueden reducir estos costes, dirección escasez de trabajadores cualificados, crear normas y fomentar la innovación. Más allá de la industria financiera inmediata, trabajando con las autoridades policiales y el gobierno puede ayudar a los bancos mitigar las tácticas cambiantes de los delincuentes financieros.

El arsenal cada vez mayor de los criminales, combinado con la incertidumbre regulatoria, está haciendo las instituciones financieras de todos los tamaños vulnerables a la actividad fraudulenta. A pesar de los nuevos métodos desarrollados por los defraudadores, tecnologías tales como análisis en tiempo real y la máquina de aprendizaje son fácilmente disponibles ahora para comenzar la remontada. Los bancos deben adoptar un enfoque proactivo que dé prioridad a la construcción de una cultura interna adecuada, la aplicación de las defensas adecuadas y colaborar con el sector en general y reguladores, para evitar la alta tecnología de adquisición y los costes de mantenimiento y atraer a los empleados con los conocimientos adecuados. Con una horda de delincuentes cibernéticos dirigidos a la riqueza y la identidad de sus clientes todos los días, nunca ha sido más importante para los bancos mantenerse al día con las técnicas utilizadas por los cibercriminales y superarlas. Sólo entonces podríamos seguir confiando en el resguardo del dinero donde exista un refugio seguro dentro de las Instituciones Financieras.

https://www.finextra.com/