Ciudad de México, 16 de mayo de 2017.

Versión Estenográfica del Panel *Cómo estar Preparado para las Amenazas de Ciberseguridad y su Impacto en la Industria de Seguros* a cargo de Fabricio Ikeda, de la empresa FICO, en el marco de los trabajos de la 27 Convención de Aseguradores organizada por la Asociación Mexicana de Instituciones de Seguros (AMIS) en el Centro Banamex.

Ciudad de México, 16 de mayo de 2017.

Versión Estenográfica de la Sesión Especializada "Cómo estar preparado para las amenazas de ciberseguridad y su impacto en la Industria de Seguros", dictada por Fabricio Ikeda, en el marco de la 27 Convención de Aseguradores AMIS realizada en el salón Diezmo 1, del Centro Banamex, en esta ciudad.

Presentador: Vamos a dar comienzo a la última plática del día.

En esta ocasión nos acompaña Fabricio Ikeda, de FICO, quien nos va a hacer una presentación acerca de Cómo Estar Preparado con las Amenazas de Ciberseguridad y su Impacto en la Industria de Seguros.

Fabricio trae una amplia experiencia, tanto en la prevención del fraude y delitos financieros, tanto para América Latina y El Caribe; tiene más de 12 años de experiencia en la industria financiera y posee lo que es una Certificación en Prevención de Lavado de Activos y una BA en Inversión y Riesgo.

Fabricio Ikeda: Bueno, muchísimas gracias.

Mi nombre es Fabricio Ikeda, como Óscar ya comentó. Gracias por tener este tipo para mirar un poco sobre ciberseguridad y por ser un tipo con cara japonesa hablando español y brasileño. Gracias por su tiempo.

La idea de la presentación de hoy es que si contestamos una de las cinco preguntas, si contestan las cuatro preguntas allá, sobre por qué debo estar preparado, qué debo hacer, cómo debo hacerlo y cuándo debe ser, ya sería un gran reto, un gran desafío vencido por nosotros.

Como hemos escuchado mucho, desde algunas presentaciones por la mañana, de algunas otras presentaciones por parte de otras personas, la ciberseguridad es un tema que está de moda.

Pero cuando ese impacto de hecho se da en la Industria Aseguradora, es lo que vamos a entender un poco.

En este fin de semana hemos visto, ustedes también han escuchado bastante, sobre este malware que es un secuestro de datos, que se llama *Wanacry* o quiero llorar y los nombres aquí son de viernes pero ya se han incrementado desde entonces.

Ahí dice que fueron 74 países, no dice la cantidad de computadoras, pero en las noticias de hoy se dice que son 150 países y 300 mil computadoras.

Ese es uno de los motivos de por qué nosotros tenemos que estar preparados con la ciberseguridad,

No solo se impactó la Banca sino también todos los tipos de industrias, inclusive hospitales; hubo hospitales en Reino Unido que cerraron sus puertas porque ya no pudieron

Hubo noticias, por ejemplo, en Brasil en donde las agencias gubernamentales también cerraron las puertas porque no pudieron más atender al público.

Creo aquí en México también hubo empresas donde apagaron los servidores, apagaron las computadoras para no tener este tipo de impacto y entonces, no cabe duda que fue un problema que impactó cualquier tipo de empresa e inclusive las Aseguradoras.

Para entender un poco de cómo podríamos prevenir este tipo de ataque, vamos a ver un poco, voy a explicar un poco cómo funciona ese tipo de software pero no de manera técnica sino que ese tipo de

software -como dijo Alejandro en la presentación anterior- afectó puramente los Sistemas de Microsoft Windows.

Impactó los Sistemas Operativos de Windows por una falla que había sido corregida en marzo de este año; o sea, si todas las computadoras tuviesen las actualizaciones hoy día o por lo menos los antivirus más actuales con una política interna de las empresas de actualizaciones forzadas, nadie iba a pasar por ese tipo de impacto.

De hecho se hicieron programas, en este caso un sistema operativo en donde hubieron algunos problemas, pero hay una responsabilidad por parte de nosotros también; hay una responsabilidad por las empresas en aplicar las políticas y una responsabilidad por nosotros, como los usuarios, de mantener todos esos dispositivos lo más seguro posible.

Esos ataques siguen creciendo a lo largo de los años, desde 2003 hasta los días de hoy; ha habido casos de fugas de información, casos de secuestro de datos y cazos de impactos en la operación de las empresas.

Para entender un poco mejor cómo impacta esto a las Aseguradoras, vemos aquí este ejemplo de *Wanacry*; no estaban muy preocupados en robar las informaciones en este tipo de ataques sino secuestrar los datos.

Ahí pedían un pago de 300 dólares para que se enviara la clave para desencriptar las informaciones.

¿Cuál fue el impacto para la empresa?

Las computadoras pararon de funcionar, los servicios pararon de ser ofrecidos y tenemos inclusive un impacto indirecto en los ingresos de esas empresas.

Lo que vemos en esta gráfica son los impactos de esos malware o de estos ataques; el business reduction, la pérdida de información por

supuesto; o sea, si robo la información para después venderla en los mercados negros y como impacto directo, la pérdida financiera también y otra vez, más informaciones de 2016, la cantidad de pérdidas que nos da a nivel mundial todos esos ataques financieros.

Lo que quiero decir es que en cuanto a la parte de las pérdidas, nosotros vemos aquí la distribución por parte de las industrias y miren el primer lugar Helfker, no es la Banca y sí Helfker, la Banca está aquí, en cuarto lugar.

Y también es asombroso ver cómo las personas saben, los defraudadores o los delincuentes buscan la punta más sensible de ser atacada o la manera más fácil de defraudar algún tipo de información o atacar alguna empresa.

En ese sentido, desafortunadamente la industria aseguradora está con un paso detrás, comparada con las otras industrias; no es el enfoque, por ejemplo, de una Aseguradora en Salud, en donde tengo que tener una solución.

Hay inclusive Aseguradoras en Latinoamérica, que ya he visitado, que ni siquiera conocen este rol de la persona, el CISO, la Chief Information Security Officer, que es la persona responsable por seguridad en las empresas.

Para explotar más ese número, vamos a ver en el caso de Salud que este es un promedio más o menos de pérdida por cliente, es lo que está diciendo acá, la pérdida promedio por cada registro.

Si estimamos en un registro -o sea, un cliente de ustedes- que hay algún problema o tengo una pérdida de 350 dólares, es fácil más o menos estimar si tengo un millón de dólares, la pérdida posible podría ser de 350 millones de dólares.

Por supuesto no vamos a impactar un cien por ciento de todos los clientes, que sea únicamente un 10 por ciento, 35 millones de dólares;

ahí están todos los costos directos e indirectos por no tener una solución de ciberseguridad.

El resumen del por qué y el mensaje, cuando salgan de aquí, es el crear conciencia que la ciberseguridad es un problema actual y la manera de trabajar o mitigar ese tipo de problema tiene que ser hecha hoy y ahora.

Ustedes dirán “Fabricio, esos números son buenos pero qué tiene que ver México” y aquí hay informaciones de México; esta de la que les voy a hablar es una noticia del 29 de marzo de 2017.

Son tan constantes los ciberataques que las Aseguradoras miraron como una oportunidad de por qué no crear Pólizas; voy a crear una Póliza de un ciberataque para tener también un ingreso para ese tipo de Póliza.

¿Pero cómo estimar, cómo especificar esta Póliza? ¿Cómo calcular un riesgo de un asegurado? ¿Cómo saber que la empresa A le voy a cobrar equis y para una empresa D será otro precio de una prima?

¿Cómo cumplir, con todos estos ataques también, este tema de la Ley de Protección de los Datos?

Inclusive si yo no cumplo -y eso tiene que ver también con la regulación- hay casos de multas que el Gobierno también ya pone como sanción a esas empresas, incluyendo Aseguradoras.

O sea, en el mercado más desarrollado como es Estados Unidos, ya hay regulaciones para que todas las empresas -incluyendo las Aseguradoras- ya tengan herramientas de ciberseguridad. Ya es una cosa en donde el mundo está caminando hacia este tipo de patrón como también el que la empresa responsable si tiene algún tipo de fuga de información, hay una penalidad, hay una multa.

Lo que está diciendo no es nada nuevo para ustedes y todo tiene que ver con la Ley de Protección de los Datos de México; he leído también

la semana pasada que hay ya reuniones del Gobierno para hacer algunos cambios y no van a cambiar directamente a la Ley de Protección de los Datos Personales sino van a agregar más cosas con esa cuestión de la ciberseguridad.

El gobierno está haciendo lo correcto. O sea, la primera precisión para que las empresas tengan la conciencia sobre ciberseguridad es la regulación.

A partir de la regulación, las empresas empiezan a invertir más y tienen esa conciencia sobre este tema antes que de hecho haya algún impacto como el de este fin de semana, con todo lo que pasó con esas empresas.

Este ya es un tema que está impactando en el mundo y está impactando también a las Aseguradoras de México y ahí contestamos o empezamos a contestar la segunda pregunta: ¿Qué debo hacer para estar preparado?

No sé si ustedes pueden ver algunas de las mejores prácticas de diversas industrias, no solo Aseguradoras:

La primera cosa que vemos es identificar cuáles son los riesgos, inclusive riesgos de cibercrímenes.

Hacer una gestión de estos riesgos, ver qué necesito como por ejemplo, quizá tener una diferencia entre riesgos estratégicos de reputación operacional, lo cual está involucrado con esta gráfica de acá, sobre cuáles son las posibles pérdidas en el caso de fuga de información y cuáles son los impactos en las ganancias.

Por ejemplo, si tengo que comprar una solución externa de ciberseguridad, si tengo que tener una persona responsable, un CISO, un Chief Information Security Officer, cuáles son los costos involucrados. Entonces ahí estamos hablando de esta gestión de los riesgos.

Políticas y procedimientos es el tercer punto allá, otra vez:

Si tengo una política y un procedimiento de actualizar todas las computadoras que tienen Windows, siete Windows 2010 o Windows que fuera, no iba a pasar este programa de *Wanacry* de este fin de semana.

Entrenamientos: ¿Cómo voy a forzar entonces a todos los empleados que actualicen o usen los dispositivos más seguros?

A través de entrenamientos, capacitaciones y la conciencia de todos.

Monitoreo y prevención.

Hay un montón de herramientas o antivirus disponibles desde firewall, son cosas que monitorean todo el tráfico de datos, todo el tráfico de información en todos los dispositivos y hacen y toman medidas o decisiones en tiempo real también. Esta toma de decisiones tiene que ser inmediata y más adelante vamos a ver uno de los motivos por lo que tiene que ser inmediata.

Asimismo hay una retroalimentación y si descubro fallas o procesos que tienen que ser corregidos, otra vez tiene que pasar por lo mismo, entender estos riesgos, capacitar a las personas y todo lo demás.

Cuando no tengo conocimiento de cómo empezar o de qué hacer, para esto están los profesionales de Seguridad; hay un montón de certificaciones disponibles en la industria de ciberseguridad, hay un montón de empresas -inclusive FICO es una de ellas- que van a ayudarles a identificar estos riesgos y qué acciones y decisiones se tienen que hacer.

Ahí empezamos a contestar lo que decía en la pregunta de cómo hacer esto; en las certificaciones utilizar ya un conocimiento que tiene la industria, pero lo más importante es concientizarla.

Creo que uno de los motivos, el que ustedes estén aquí y ahora, sería esta preocupación ya de la ciberseguridad; qué tengo que hacer, qué está haciendo la industria, cuáles son los impactos para mí y ahí estamos hablando de concientizar sobre ese tema que es un tema nuevo hoy en día pero es un tema que ya nos impacta a todos nosotros.

Hay algunos casos no solo de Aseguradoras sino cualquier tipo de empresa, donde empieza la creación de este rol que había comentado antes, que era el CISO, Chief Information Security Officer, para que sea una persona responsable por todo ese tema de la ciberseguridad.

Aquí no se puede ver pero lo que quiero decir con este organigrama acá es que el CISO ya va a reportar directamente al CEO y no más bajo un equipo de auditoría, no más bajo un equipo de operaciones, un equipo de tecnología porque para que no tenga conflictos de intereses.

Ya he visitado muchos Bancos, inclusive no solo CISOS sino también la persona de cumplimiento; estaba debajo, reportaba con una persona de ventas.

¿Entonces cuáles son los intereses que tengo que aplicar para quizá limitar un poco algunos tipos de productos tomar decisiones y si esto va a impactar directamente las ventas y operaciones?

Ahí hay conflictos de intereses. En ese sentido, es una de las mejores prácticas que la industria también está aplicando.

Para responder la pregunta de cómo hacerlo, les comento que cuando hablamos de ese tema de ciberseguridad, estos son los pasos más comunes: Prevenir, detectar, investigar, responder, predecir y prepararme.

Aquí hay algunos ejemplos de herramientas, políticas y soluciones que más suelen ser utilizadas.

En el caso de prevención, tener una seguridad de la red, sea a través de firewalls u otras herramientas; aun también sobre la identidad de los usuarios, de accesos de usuarios, contraseñas y todo eso.

Herramientas inclusive para identificar los malware, que lo que hacen es monitorear todos los datos; inclusive creo que ustedes también pueden tener los datos monitoreados y ni siquiera saben que están siendo monitoreados.

Algunas empresas de telefonía ya lo hacen, las empresas lo hacen; inclusive este teléfono que es de FICO también ya lo tiene acá, está como escondido pero también lo hace.

O sea, todos los datos que pasan por aquí son monitoreados para impedir ese tipo de amenazas y hay softwares ahí, hay herramientas que se llaman Defensa Trade Detection para esto.

No sé si ustedes me han escuchado esto de los SINCS pero también hacen lo mismo: Es tener en un servidor o en la nube herramientas que van a mantener todos los datos de las computadoras.

También hay siempre una solución, un aplicativo instalado de manera escondida en las computadoras que están enviando esos datos para las empresas y hay algunas veces que esta herramienta está pegada en los firewalls o en los servidores de comunicación de las empresas.

Estas son las herramientas como los antivirus y que también tienen un control, sobre todo en la navegación que hacen las personas.

¿Pero cómo utilizar mejor esto?

Hemos hablado bastante de esa transformación digital, hemos hablado sobre ciberseguridad, hemos hablado inclusive de inteligencia artificial, sobre Machine Learning.

Una cosa que nosotros en FICO estamos haciendo y también la industria es la analítica aplicada para ese tema de ciberseguridad

porque no es solo tener un CEO, no es solo tener conjunto de reglas para identificar esos perfiles sino tener la analítica aplicada, tener inteligencia artificial o Machine Learning aplicada a ese tema de ciberseguridad.

Aquí cabe decir que los datos, desde Big Data o cualquier tipo de datos, son datos que pasan por un servidor, que pasan por cualquier dispositivo pero no te da la información.

¿Qué tengo que hacer con ese dato, porque hay un montón de datos?

Imagínense -por ejemplo- este wifi de este evento, la cantidad de datos que pasaron por un ruteador o por un dispositivo como servidor solamente el día de hoy, solamente en este último minuto.

Cómo tener una inteligencia de saber que de hecho estamos hablando de un ataque como este *Wanacry* o sea solamente una persona que se vio en el Facebook.

¿Cómo distinguir si de hecho es un ataque, si es un acceso genuino? ¿Cómo distinguir que un empleado está accediendo a una información indebida, que no tiene permiso para hacerlo o inclusive el que un gerente que de hecho esté haciendo lo correcto?

Hay un montón de datos, gigabytes o terabytes por minutos, por segundo, cuando estamos hablando a nivel más nacional y ahí entra inteligencia artificial porque un ser humano, una persona no tiene la capacidad de hacerlo pero la analítica sí tiene esta capacidad.

En ese sentido, hemos -y cuando digo “hemos” sería la industria y obviamente con FICO- creado esos scores que básicamente es dejar de manera más transparente el uso para una persona de seguridad o inclusive para los Directores de Tecnología porque yo no voy a explicar en bytes qué está pasando pero tengo que dar una información lo más precisa diciendo “esto pasó, esta fue la acción que tomamos” y también lo que debemos hacer para evitarlo en el futuro.

Los scores básicamente resumen todo esto y empezamos ahí a entender un poco mejor que si soy una Aseguradora y estoy analizando una prima de ciberseguridad; si voy a conceder, si voy a otorgar una póliza para una empresa que están pidiéndome, una póliza de ciberseguridad, ¿cómo hacer el precio de esto, cómo estimar el riesgo por detrás?

FICO ya tiene consolidada en la industria, score que te da la capacidad de pago de la persona, que te da la capacidad crediticia de la persona, cuál puede ser un poco el riesgo de esta persona, de esta empresa, pero no tiene nada qué ver con ciberseguridad.

Una herramienta, una solución que hemos visto en la industria que está creciendo ahora sería “yo puedo dar también cuál es el score de esta empresa o de este posible asegurado en términos de ciberseguridad”.

Al final del día, se trata de que la Aseguradora va a tener un score como FICO Shure Score sobre cuál es el mejor precio para dárselo a esa empresa basado en todo un historial crediticio, basado en un montón de informaciones como ya hemos visto en las presentaciones anteriores, pero también cuál es la probabilidad o cuál es el riesgo de exposición de esta empresa en términos de ciberseguridad.

Podremos saber cuál es la probabilidad de que el día de mañana esta empresa que estoy asegurando va a sufrir un ataque cibernético o va a sufrir una fuga de información. Este es el primer paso para entender cuál es el riesgo de la empresa a la que estoy otorgando esta Póliza de Seguro.

Como Aseguradora, no solo miro los términos de Pólizas sino también debo entender cuáles son mis riesgos o mi exposición a niveles de seguridad. Ahí sería como si fuera una herramienta con cien pero combinado con analítica también.

Inclusive hay un concepto que es un cuadrante mágico que se llama UEBA, que significa User and Entity Behavior Analytics; o sea, voy a

ver perfilar los usuarios a través de todos los datos que son traficados por la red e identificar si un acceso el login de Fabricio -por ejemplo- de hecho es un acceso genuino o si está pasando ataque con alguien, haciéndose pasar por Fabricio haciendo cosas que no debe hacer.

Entonces identifico las entidades, los usuarios, los accesos y en tiempo real identifico si hace un ataque o no; eso tiene que ver con este concepto de UEBA.

Si tengo que estimar cuál es el riesgo, tengo que tener los rangos, los umbrales para comparar esta empresa con otras; o sea, si voy a asegurar una panadería porque esta panadería quiere estar como que preparada para un ciberataque, ¿cuál es el impacto para las panaderías de México?, ¿cuál es la exposición de esta panadería con relación a la industria?

Entonces, en este concepto, nosotros comparamos la Data con toda la Data de la industria y generamos ese score que va a ayudar en esta decisión. Ustedes ya ofrecen este tipo de Póliza para un ciberataque.

Para contestar una de las últimas preguntas, sobre cuándo debemos hacer o cuándo debemos empezar a mirar ese tema de ciberseguridad, el tiempo es ahora.

Lo que vemos en esta diapositiva es muy claro: Un ataque para comprometer algún tipo de información, solamente se tarda como que segundos, minutos, en algunos casos horas; este caso de este fin de semana fue un ejemplo de esto.

O sea, en un par de días impactar 300 mil computadoras no es nada fácil pero el tiempo para descubrir esos ataques o tomar un tipo de decisión, el promedio es de días, semanas, meses o años.

O sea, si no estoy listo para detectar esos problemas, tampoco voy a tener tiempo para hacer alguna cosa, para prevenir ese tipo de ataques y un 54 por ciento de estos problemas de fuga de información, de los Data Breaches ni siquiera son descubiertos.

Hay una frase que es bastante común en esta industria de ciberseguridad que es: Hay dos tipos de empresas: una empresa que sí sufrió un ataque y el otro tipo que ni siquiera sabe que sufrió un ataque.

O sea, todos nosotros estamos como que susceptibles a este tipo de ataques.

Para terminar, los takeaways o los conceptos fundamentales que ustedes se deben llevar a casa o para la empresa, o que tengan un poco de miedo a partir de ahora, pues es un tema de moda pero es un tema que puede impactarlos, es que todo tiene que ver con concientizar sobre ciberseguridad; empezar desde ya a entender cuáles son los riesgos.

Hay un montón de maneras de cuantificar, tener un tangible en terrenos de riesgos; yo les di un ejemplo que es la pérdida de más o menos 300 dólares por persona, habría solamente que multiplicar por la cantidad de registros o de clientes que ustedes tengan.

Hay que empezar desde ya a hacer un monitoreo y prevención sobre este tema; si no hay un CISO, si no hay una persona responsable por ese tema de ciberseguridad, tienen que empezar desde ya a plantear ese tema.

Por supuesto no quiero solamente invertir y tener gastos con ese tema de ciberseguridad, pero hay nuevas oportunidades; si nadie que está aquí ofrece una Póliza de ciberataque, podría empezar desde ahora también hoy a ofrecer este tipo de Póliza.

Es una oportunidad de la industria que tiene que ver con otra palabra llave de esta conferencia, que es un mercado disruptivo; o sea, cada día hay nuevas oportunidades, buenas para unas empresas, malas para otras y aquí es mirar una oportunidad de negocio que es empezar ahora a tener esta Póliza para ciberataques.

Quiero comentarles que FICO ya tiene consolidada a la industria aseguradora y otras industrias también con soluciones de fraude y cumplimiento en ciberseguridad.

Si quieren más información, aquí pueden ver más detalles sobre lo que ofrecemos para la industria aseguradora y otras industrias, mis contactos y también estaríamos aquí por si al fin de la sesión tienen algún tipo de preguntas o inquietudes.

Presentador: Muchas gracias, Fabricio; una presentación bastante interesante y creo que ahora mismo de preocupación para todos los que estamos aquí.

No sé si hay alguna pregunta, aprovechando que tenemos aquí a Fabricio.

Pregunta: Buenas tardes, gracias por la presentación.

No sé si tengas la estadística sobre cuánto yo debo de estar invirtiendo como empresa, en proporción a mis ventas, para saber si estoy haciendo la correcta designación de recursos al tema de ciberseguridad.

¿Habría una estadística de que si vendo cien pesos debo de estar, por lo menos, teniendo un peso destinado a esto o tomando como escala las que tienen una buena práctica, para saber si estoy dentro de la métrica o no le estoy designando recursos a ello?

Fabricio Ikeda: No hay un porcentaje exacto, pero para identificar ese porcentaje va a depender de saber cuál es mi riesgo.

Hay inclusive certificaciones, sabemos certificaciones que hace CIACP que dice que si tengo un millón de dólares invertidos en servidores, este es mi riesgo de exposición; si tengo algún tipo de problema con esos servidores, sea por un ataque cibernético o cosas así, voy a perder un millón de dólares.

Entonces yo identifico que mi exposición es de un millón de dólares pero sabemos que los servidores, a lo largo de los años, van a perder un poco de los valores y un año después, esos servidores ahora van a valer 500 mil dólares.

Antes yo estaba invirtiendo en ciberseguridad cien mil dólares para proteger un millón de dólares de servidores; en el año siguiente voy a seguir invirtiendo cien mil dólares para proteger 500 mil dólares y entonces esta matemática va a depender mucho de esto pero no hay un porcentaje. Cada empresa tiene un porcentaje de acuerdo con su apetito de riesgo.

Presentador: Yo voy a aprovechar para hacer una pregunta.

Comentabas de la figura del CISO, que yo coincido que es muy importante disponer de él en todas las organizaciones.

¿En organizaciones que todavía no cuentan con esta figura, qué tan válido es -bajo su experiencia- que sea un externo el que realice esta función?

Fabricio Ikeda: ¿Mi opinión?

Presentador: Sí, la real.

Fabricio Ikeda: Que no sea una persona externa sino otra persona pero que tenga ese rol de CISO; que sea un Chief Risk Officer pero que tenga este rol de CISO también porque este CISO va a tener responsabilidades de tener un plan de seguridad, de definir las políticas internas, de definir -por ejemplo- la comunicación entre las personas de más nivel técnico y la Junta de Directores.

Entonces es mejor que sea una persona interna con este rol, pero es difícil; o sea, es difícil que un Chief Risk Officer tenga la formación necesaria para un CISO. Ahí sí tienen que utilizar por lo menos una experiencia externa para empezar a crear esta cultura de manera

interna, para que en el futuro sí se genere una persona interna con este rol de CISO.

Presentador: No sé si hay alguna pregunta más.

Bueno, pues muchas gracias de nuevo Fabricio.

- - - 0 - - -