ULACIT

INVESTIGACIÓN EMPRESARIAL APLICADA (FINANZAS)

PROFESOR:

CÉSAR PABLO ENRÍQUEZ CARUZO

¿CUÁL ES EL IMPACTO FINANCIERO DE UN FRAUDE ELECTRÓNICO QUE PUEDE EXPERIMENTAR UNA ENTIDAD FINANCIERA Y QUÉ MECANISMOS SE PODRÍAN IMPLEMENTAR PARA EVITARLO O REDUCIR LAS REPERCUSIONES?

JORGE BETANCOURTH VEGA

1-0916-0147

2009

Índice

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Tabla de Ilustraciones

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Resumen

Este artículo aborda el tema de los fraudes electrónicos con el propósito de aclarar la definición de estos, qué los causa e identificar las diversas formas en que se pueden llegar a implementar. Se muestra la pérdida económica que ha venido representando, en el tiempo, la fuga de información, así como también la cantidad de registros que se han visto comprometidos año tras año. Con esto, se pretende alertar tanto a las personas físicas como a las jurídicas al mostrar el posible impacto que pueden llegar a sufrir; a la vez que se presentan posibles opciones que merecen un estudio más profundo para evaluar la factibilidad y la necesidad de su implementación con el fin de prevenir y/o reducir el impacto económico de los fraudes.

Palabras clave

Fraude electrónico, fuga de información, prevención, PCI DSS, Cobit

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Abstract

This article addresses electronic frauds with the purpose of clarifying their definition, root causes and identifying different ways in which they can be implemented. It shows the economic impact data breaches have represented along the years as well as the number of compromised records. Pretends to bring perspective to people as well as to companies by showing the impact they might suffer while pointing out different options that deserve a deeper evaluation in order to determine implementation feasibility and necessity with the purpose of preventing or reducing the economic impact.

Keywords

Electronic fraud, data breach, prevention, PCI DSS, Cobit

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Introducción

El fraude electrónico no es una situación reciente, este se viene presentando desde la introducción de los medios electrónicos para realizar las transacciones financieras y es básicamente, un paso en la evolución de los fraudes realizados en el mundo físico.

Originalmente, fueron considerados como normales e incluso llegaron a ser llamados “el costo de hacer negocio”, pero el crecimiento acelerado y el impacto que ha llegado a representar han hecho que el mundo torne sus ojos hacia ellos y se organice para combatirlos. Día tras día, los fraudes son más elaborados, por tanto, los mecanismos de detección, prevención y corrección deben tratar de ser mejores para reducir el impacto que se pueda sufrir.

El fraude electrónico

Concepto

El fraude electrónico, como todos los otros tipos de fraudes que existen, busca colocar a la persona que efectúa el acto en una posición en la que pueda obtener un beneficio personal de alguna manera.

Este, como todos los crímenes, es el producto de tres factores: la motivación para efectuar el fraude, la presencia de una víctima potencial y la ausencia de un guardián capaz de detenerlo.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

A medida que se fue avanzando en el desarrollo de la tecnología, se fue gestando una amplia gama de beneficios para la humanidad; pero a la vez, se potenció de maneras antes nunca imaginadas la capacidad y los medios para poder sacar provecho de otras personas o empresas.

Una de estas maneras es la no presencia física en el mundo digital, lo cual permite que a través de diversos mecanismos se pueda engañar a otros, haciéndolos pensar que cierta información es verdadera con la finalidad de obtener otra que sí lo es y que eventualmente, podría ser utilizada para obtener fondos de manera ilícita a través del uso de robo de identidad. Para esto, se explotan vulnerabilidades en las aplicaciones instaladas en los equipos, deficiencias que la persona que está siendo víctima, ni siquiera sabe que tiene. La era digital también posibilita que los criminales se comuniquen entre ellos de manera secreta, alteren documentos utilizando herramientas de alta tecnología y manipulen sistemas de pago electrónico, para obtener fondos de manera ilegal

¿Por qué surgen los fraudes electrónicos?

En el pasado, los grandes robos de la historia sucedieron en los bancos; pues en ese tiempo eran el lugar donde se encontraba el dinero y esto atraía a malhechores, como el famoso Willie Sutton, en los años 30.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

La incidencia de estos robos a bancos en el mundo real, los avances tecnológicos y la búsqueda por disminuir el costo promedio, por transacción, al mover a los clientes a usar canales de distribución más económicos, han impulsado a las entidades financieras a promover fuertemente las transacciones electrónicas al punto en que, en algunos países, se mueve mucho más dinero electrónicamente del que se mueve en moneda física.

Al darse este cambio en la manera de mover el dinero, el sitio en donde "el dinero está" cambió de lugar e hizo que los criminales voltearan su mirada hacia el mundo digital, para estudiarlo y encontrar un gran potencial al hallar vulnerabilidades que podían explotar en los diferentes componentes presentes, tanto los lógicos como los físicos; además de contar con la conveniencia que brinda la "impersonalidad" ya mencionada del medio, así como también el crecimiento tan acelerado que ha tenido la penetración de la Internet y de otros tipos de negocios que han incursionado en el ambiente en línea.

Según agencias, como la APWG ("*Anti-Phishing Working Group*") y la ITRC ("*Identity Theft Resource Center*"), la cantidad de fraudes ha venido en aumento con los años, para alcanzar tasas de crecimiento de cerca de un 50%, de un año a otro. Con esto sobre la mesa y la situación económica que vive el mundo actualmente, las empresas deben empezar a poner atención a lo interno; pues la motivación que tiene una persona para cometer un fraude crece en tiempos de crisis. Las empresas deben dirigir esmerada observación al riesgo que la organización enfrenta con sus empleados, estos típicamente tienen los accesos a la información y el conocimiento para cometer un fraude, pero no poseen la motivación.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Los criminales, por el contrario, tienen la motivación; pero no necesariamente, las herramientas o el conocimiento para propiciar una fuga de información. Al presentarse una intersección entre los grupos anteriores es cuando se está ante un peligro real; pues se está propiciando un empleado con accesos, herramientas y además, la motivación por generar una fuga de información, dada quizás por una mala situación económica por la que se pueda estar pasando. Dado esto, el hecho de que la economía entre en un período de recesión puede ser considerado como un disparador más que puede potenciar los fraudes electrónicos.

Formas en las que se puede llevar a cabo un fraude electrónico

Existe una gran diferencia entre la manera en que las personas y empresas perciben los fraudes electrónicos y las formas en que estos se pueden llegar a presentar. Es importante revisar cuál es la manera en que las personas están recibiendo información sobre este fenómeno y cuáles son las otras formas en que se puede llegar a presentar.

¿Cómo interpretan las empresas que pueden sufrir un fraude electrónico?

Para beneficio de los criminales, son muchas las personas, tanto físicas como jurídicas, que tienen una noción equivocada de las maneras en como se puede llevar a cabo un fraude electrónico.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Debido a la falta de educación en relación con el tema, son muchas las que consideran que un fraude electrónico puede ser llevado a cabo únicamente, por un malhechor o un grupo organizado con grandes recursos, el cual logra quebrar la seguridad de los sistemas, a través de dispositivos tecnológicos de avanzada, de supercomputadoras y de un ingenio sobresaliente.

Considero que este pensar se ha generado mucho, por la imagen que han posicionado las grandes filmaciones de Hollywood en relación con el tema desde hace varios años, en las que se logra obtener grandes cantidades de dinero irrumpiendo en los sistemas de las empresas, buscando debilidades en estos y explotándolos.

A manera de ejemplo, algunas de las películas que han logrado cavar esta imagen en el pensamiento de las personas son: WarGames (1983), Sneakers (1992), Hackers (1995), The Net (1995), 23 (1998), Enemy of the State (1998), Pirates of Sillicon Valley (1999), Takedown (2000), AntiTrust (2001), SwordFish (2001) y The Italian Job (2003).

Pienso que estas y otras producciones han inculcado una idea muy limitada en las personas, para que estas lleguen a pensar que ellas o sus compañías están exentas de este tipo de ataques, al no representar un reto o un premio importante para los criminales.

Esto debe llegar a cambiar, las personas deben saber que al utilizar medios electrónicos para hacer tareas en su día a día, están expuestas a ser víctimas de un fraude electrónico, en cualquiera de las formas en que este se presente.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Otras formas de implementar un fraude electrónico

No quiere decir que la manera que representa Hollywood en sus películas no se pueda dar, sino que además de esta existen otras más del día a día, con las que se cometen fraudes electrónicos; entre estas se encuentran:

Fraude interno

Este es el que se comete, cuando un empleado de una empresa abusa de su poder para obtener un beneficio propio o hace uso de herramientas o accesos internos, para con esto enriquecerse ilícitamente; debido a esto es importante disponer de políticas de "conozca a su empleado", para de esta manera poder determinar cuándo se manifiesta un cambio en su comportamiento.

Ingeniería Social

Es el proceso mediante el cual se convence a alguien de ejecutar acciones o divulgar información confidencial. Llevar a cabo este tipo de fraude es mucho más sencillo que romper la seguridad de un sistema.

Las técnicas para efectuar este tipo de fraudes van desde las muy sencillas, como hacerse pasar por alguien más, hasta técnicas más sofisticadas.

Según Gartner, muchas de las fugas de información más perjudiciales han sido debido a la ingeniería social y no a un hackeo.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Phishing

El phishing consiste en suplantar la identidad de una persona o empresa reconocida, haciendo creer a la persona que está siendo atacada que está ingresando al sitio oficial de dicha empresa, con la finalidad de obtener tantos datos como sea posible de la víctima para su posterior uso con propósitos fraudulentos; este tipo de ataque podría incluso ser considerado como un tipo de ingeniería social dado que el delincuente, basándose en engaños, trata de obtener datos que no le competen.

Existen varias maneras de realizar este tipo de fraude, entre ellas están: a través de un mensaje corto de texto o SMS, de una llamada telefónica, de una página web, de una ventana emergente que tiene mucha similitud con el sitio web oficial de una empresa o por medio de un correo electrónico que solicita datos o que tiene un enlace al sitio falso.

Troyanos

Los troyanos constituyen programas que simulan ser aplicaciones útiles, pero que dentro de su código poseen funciones con otra finalidad. Reciben este nombre por la similitud con el mítico caballo de Troya, con el cual los griegos dominaron esa ciudad. Muchos de estos tienen como propósito recabar información o abrir puertos de entrada a la computadora, con lo cual esta queda expuesta y puede ser accedida remotamente, por el malhechor para obtener datos con los cuales puede llegar a efectuar un fraude financiero.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

KeyLoggers

Un keylogger es un tipo muy específico de troyano, y su finalidad es la de recolectar información ingresada en el sistema. Se encarga de registrar las pulsaciones hechas desde el teclado, con el fin de almacenarlas y luego enviarlas a un delincuente.

Con el uso de este tipo de herramientas, los malhechores lograr averiguar las contraseñas que las víctimas digitan para entrar a sus "sitios seguros", así como también el identificador del usuario, para dejar así completamente expuesta la seguridad de un alto porcentaje de sitios financieros, cuyo esquema de protección consiste únicamente en estos dos componentes.

ScreenLoggers

En un paso más avanzado que los keyloggers, se encuentran los screenloggers que son también troyanos; pero que tienen la capacidad de grabar las acciones que se están efectuando en la pantalla; de esta manera, se puede romper la seguridad de sitios que ofrecen esquemas de acceso en los que se utilice el mouse, para digitar una contraseña, o en los que se muestre una imagen que el usuario debe reconocer o una serie de números que se seleccionen con este dispositivo.

Sniffers

Los sniffers representan aplicaciones que pueden llegar a un equipo, a través de la descarga de troyanos, y el propósito de ellos es revisar todo lo que está transitando en la red en que se encuentra un equipo.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Estos programas pueden causar mucho daño a una empresa, pues muchas veces las empresas se preocupan por asegurar los datos dentro de los equipos, pero no contemplan que estos viajan por la red y en aquí es donde pueden ser vulnerables. Para mostrar el impacto del fraude, que se puede causar con este tipo de aplicaciones, se comentará más adelante sobre el monto al que llegan las pérdidas de la que es considerada la fuga de información más grande de la historia, acontecida durante el 2008 y principios del 2009; la que ha llegado a sumar más de 13 millones de dólares y aún no se termina de medir el impacto.

¿Quiénes se ven financieramente impactados y en qué nivel?

Originalmente, los fraudes eran considerados como un costo más para las empresas, pero el impacto de los crímenes económicos ha venido en aumento exponencial a lo largo de los años hasta llegar al punto en el cual, ya no se puede pensar en ellos como "el costo de hacer negocios", sino más bien como en una potencial crisis para una nación.

En el medio electrónico, el ruido que se causa por los crímenes económicos es tanto, que este no permite desarrollar todo el potencial de Internet al encontrarse con usuarios o clientes con un nivel de confianza conservador.

Para el 2001, según Gartner, el número de fraudes con tarjetas de crédito era 12 veces más grande en Internet, que en el mundo físico. Si vemos el mundo de las fugas de información, el número anterior se ha venido potenciando con el tiempo, y el factor más representativo es el número de registros que se ven comprometidos en dichas fugas.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Fugas Electrónicas versus Fugas en mundo real					
(2008)					
Electrónicas					
	Número de fugas	540		Número de registros	35,125,425.00
	Porcentaje de las fugas	82.3		Porcentaje de los registros	98.4
Mundo Real					
	Número de fugas	116		Número de registros	565,830.00
	Porcentaje de las fugas	17.7		Porcentaje de los registros	1.6
Fugas totales: 656					
Registros comprometidos : 35,691,255					

Tabla 1: Relación entre fugas electrónicas y fugas en el mundo real (2008). Fuente: ITCR (idtheftcenter.org)

Según el instituto Ponemon, las fugas de información son cada vez más costosas, un ejemplo de esto se muestra en la figura 1 en la que se ve que, entre el 2006 y el 2008, se presentó un incremento de un 11% en el costo promedio, por registro comprometido. Cabe destacar que este costo promedio incluye tanto los gastos directos, la detección, la mitigación y la respuesta ante la fuga, como los gastos indirectos en que se incurre con una fuga de información, en la que los problemas con los clientes son los más representativos.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

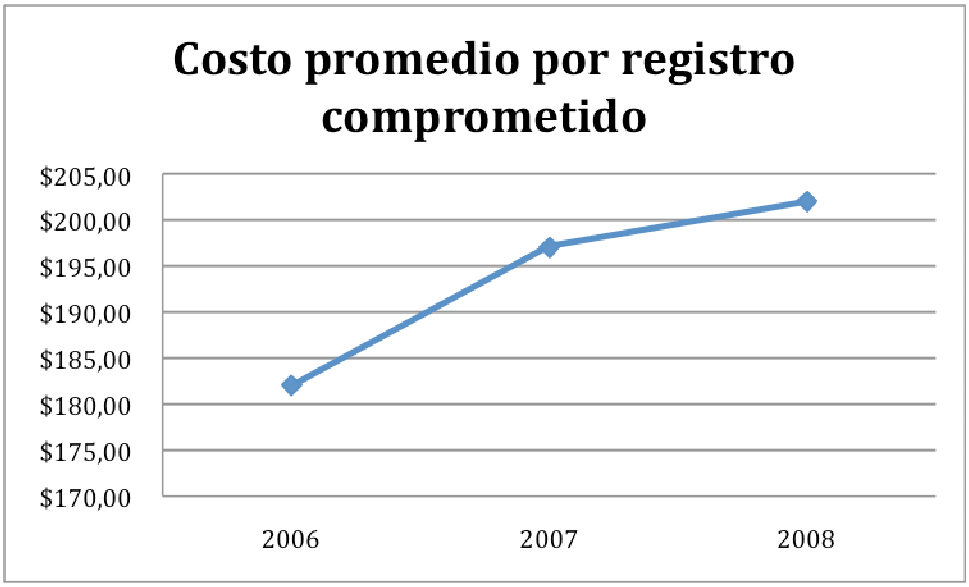

Figura 1: Costo promedio por registro comprometido.

Fuente: Instituto Ponemon - 2009

Teniendo en cuenta los datos anteriores, es necesario tomarle la importancia necesaria a la protección de los registros que toda persona y empresa mantiene, pues las pérdidas potenciales son muy altas.

Impacto a personas físicas

Cuando una persona física sufre un fraude electrónico, le puede repercutir en el estatus de crédito que maneja ante los sistemas bancarios, o puede perder dinero o activos, a través del fraude como tal o como consecuencia de este, y por supuesto, perder su privacidad.

Para una persona física, una de sus mayores preocupaciones es el nivel percibido de seguridad que le ofrecen las empresas con las cuales hace negocios, dado que una fuga de información en estas puede traerle repercusiones personales como las mencionadas.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

En una encuesta llevada a cabo por la ACB (“*America´s Community Bankers*”) en el 2007, a 181 de sus miembros, se encontró que el 70% había tenido que reimprimir 3 veces o más las tarjetas de crédito a sus clientes y el 30% restante, 5 veces o más.

Esto representa un impacto enorme para los clientes, debido a que tienen que estar dejando de lado su vida normal al ver que sus tarjetas de débito y crédito son canceladas para ser impresas de nuevo, lo que mina la confianza en el emisor e incluso, en el medio de pago como un todo.

Impacto a personas jurídicas

Las personas jurídicas pueden sufrir de maneras diferentes, a las que sufre una persona física al enfrentarse a un fraude electrónico, desde ataques para dejar el servicio inestable o sin respuesta, virus de computadoras, o acceso inautorizado a información sensible. Estas pasan por pérdidas de ganancias, pues deben honrar los compromisos con sus clientes indiferentemente, hayan perdido o no dinero. Además, pueden enfrentar problemas de reputación o imagen pública, con lo cual se puede perder clientes y poner en riesgo la continuidad del negocio. Otro tipo de impacto puede ser el de las pérdidas de propiedad intelectual. Según la asociación de evaluadores de fraude certificados, para el 2001 en Estados Unidos, una organización promedio llegaba a perder hasta un 6% de sus ganancias anuales por fraudes, perpetrados por sus propios empleados.

Entre los costos potenciales generados por una fuga de información, se encuentran:

- La pérdida de negocio (en el corto y largo plazo, debido a una pérdida de reputación).

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

- El costo de las actividades relacionadas directamente con el encontrar y corregir la fuga de información.

- El costo potencial de las demandas legales de los clientes y proveedores.

Si bien es cierto que todas las empresas sufren de fraudes electrónicos indiferentemente de su tamaño, quizás las más afectadas son las pequeñas; pues al no poder costear los equipos necesarios para detectar el fraude, sufren de ataques más severos que en muchas ocasiones las saca completamente del negocio, debido a las pérdidas que enfrentan.

Ahora bien, la cantidad de empresas que han sido víctimas de fraudes y el impacto de estos es solo una porción de lo que en realidad sucede, debido a temas de comunicación; pues en muchas ocasiones, las empresas no reportan dichos fraudes por temor a dañar su reputación o la confianza de sus clientes y accionistas. Esto se manifiesta desde hace algunos años, ya en el 2002 en una encuesta del FBI y el Instituto de Seguridad de Computadoras encontraron que el 80% de los entrevistados aceptaba haber tenido pérdidas financieras, pero solo el 44% estaba dispuesto a cuantificarlas.

Esta falta de reporte es hasta cierto punto entendible, aunque no justificable, ya que se debe tener claro que la percepción que tienen los inversionistas, accionistas y clientes del desempeño actual y futuro de una empresa contribuye en gran parte a materializar la diferencia entre el valor contable de las acciones y el valor en que se negocian en los mercados financieros, juntándose esta percepción con factores como las razones económicas y los cálculos financieros.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Una percepción positiva es delicada de mantener y es una variable de suma importancia, pues la pérdida de confianza puede provocar que una empresa desaparezca y esta es una pieza clave en el desarrollo y crecimiento de las empresas, como se aprecia en la figura 2.

Desgraciadamente, un fraude electrónico puede llevar a la pérdida de credibilidad en una empresa, y cuando sucede esto, se están minando las bases de su reputación, con potenciales repercusiones devastadoras. Se pude tener muy buena visión, productos y servicios; pero sin clientes, no hay insumos para que la empresa produzca bienes.

Figura 2: Templo reputacional. Fuente: Espiñeira, Sheldon y Asociados

En el caso expuesto anteriormente, sobre la encuesta de la ACB, además del problema de reputación que esto representa y la pérdida de confianza de los clientes, cabe destacar que el reimprimir una tarjeta le cuesta a un banco cerca de $15.00 y hacer esto con la gran cantidad de clientes y las veces que se tiene que hacer, implica sumas representativas que pueden poner las cifras de la empresa en números rojos.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Frecuencia de los eventos

En relación con las fugas de información, si bien es cierto que el sector financiero, bancario y de crédito ha permanecido como el más proactivo, en lo que a protección de datos se refiere, este tiene cantidades importantes de fugas de información.

En la tabla 2 se muestra el crecimiento que se ha venido gestando en cada una de las industrias para los últimos tres años, en ella se puede observar cómo el sector militar pasó, de tener el crecimiento más alto en el 2006, a estar en un tercer puesto para el 2008 y cómo el sector financiero efectivamente, se ha mantenido como "el más protegido".

Fugas de información en el 2008				
	Número de fugas	2008	2007	2006
Negocios	24	36.6%	28.9%	21.0%
Educación	131	20.0%	24.8%	28.0%
Gobierno/Militar	110	16.8%	24.6%	30.0%
Salud/Médico	97	14.8%	14.6%	13.0%
Financiero/Crédito	78	11.9%	7.0%	8.0%

Tabla 2: Incremento de fugas de información por segmento. Fuente: ITRC (idtheftcenter.org)

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

La cantidad de fugas de información va en aumento cada año. Para el 2008, se presentó un incremento de un 47% en la cantidad de fugas, y pasó de 446 a 656; esto, por tanto, repercute en la cantidad de pérdidas monetarias que se enfrentan mundialmente por este fenómeno.

Acciones correctivas y preventivas ante un fraude electrónico

Todas las personas que realizamos transacciones, por medio de canales electrónicos, estamos propensas a sufrir de un fraude de este tipo.

Indiferentemente, del posible impacto que este pueda llegar a representar para nosotros o para nuestras empresas, existen una serie de acciones que se pueden efectuar ya sea para prevenir o para aminorar el posible impacto de esta situación.

Tanto en el ámbito personal como en el jurídico, es imperativo tomar acciones como las siguientes para disminuir la probabilidad de ser una víctima de los ladrones electrónicos:

- Proteger el computador o las computadoras con las cuales se trabaja, manteniendo actualizado tanto el antivirus como el sistema operativo
    - Hace algunos años era muy poca la población que tenía preocupación por la seguridad de sus equipos, pues estos se encontraban de una u otra forma "aislados" del mundo y el intercambio de archivos, se hacía por medios convencionales como los disquetes. Para la realidad de hoy en día, con la globalización y la penetración de Internet en aumento en el mundo, se hace

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

extremadamente peligroso operar un equipo sin los sistemas de seguridad apropiados y actualizados que estén revisando toda comunicación o archivo que intente llegar a un equipo. En la actualidad, los disquetes prácticamente desaparecieron y mucha comunicación se transmite, incluso, por medios inalámbricos que están expuestos al público; por tanto, es una necesidad tener los sistemas detectores de virus y troyanos al día y activos todo el tiempo que el equipo esté encendido.

- Las personas muchas veces creen que, cuando adquieren un sistema operativo para su equipo y un antivirus, están protegidos contra un ataque; pero, olvidan que estas aplicaciones son programadas por personas que están propensas a cometer errores y que hay miles más, que se dedican a buscar y explotar estos errores o vulnerabilidades en los sistemas, para su propio bien. Por esta razón, así como se mencionó que se debe actualizar el antivirus, se hace necesario estar instalando las actualizaciones del sistema operativo que sean liberadas por el fabricante de este; pues en muchas ocasiones, estas vienen a cerrar "portillos" que por una u otra razón quedaron abiertos y están proclives a ser explotados.

- Proteger el uso de las contraseñas de los sistemas que utiliza.

    - Hay quienes creen que los sistemas exigen contraseñas con combinaciones de números y letras y con una longitud determinada, solo para hacer las cosas difíciles; pero es necesario entender que las contraseñas se solicitan de

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

esta manera, para que a un delincuente le sea más difícil averiguarla. Hay que inculcar en la cultura personal y organizacional, que las contraseñas son personales e intransferibles y que en el momento en que se comparta esta con otra persona, el riesgo de sufrir un fraude empieza a aumentar.

- Las aplicaciones y sitios generalmente, otorgan una contraseña por defecto para iniciar con su uso; se ha de estar claros de que estas deben ser cambiadas, tan pronto sea posible; ya que típicamente, estas contraseñas que se dan por defecto son de conocimiento público o sencillas de obtener.

- Tener conciencia del sitio desde el cual se está accediendo a las aplicaciones

  - Con la llegada de los cafés con acceso a Internet y de la tecnología inalámbrica, no cabe duda de que la facilidad de acceso a los sistemas aumentó; pues prácticamente, desde cualquier localidad se puede acceder a los sitios personales; por eso, ahora hay que estar consciente de que esos sitios y accesos inalámbricos generalmente, no cuentan con las medidas de seguridad necesarias para preveer un ataque elaborado y que es factible que alguien esté utilizando programas sofisticados, para "escuchar" todo lo que este viajando por la red, cuando se establece una conexión; averiguando de esta manera usuarios, contraseñas, números de tarjetas de crédito y demás. Dado lo anterior, se debe tener mucha precaución al utilizar los sitios públicos de acceso a Internet; pues al hacerlo, podríamos estarles entregando a los malhechores, "las llaves" de los sitios que usamos. No todos los sitios

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

los deberíamos acceder desde todas las locaciones posibles y si se hace esto, se ha de tener la costumbre de “desconectarse” del sitio por el mecanismo que este provee; en lugar de simplemente, apagar el equipo o cerrar la aplicación, ya que esto puede dejar valores activos en la memoria del computador.

Mi empresa sufrió, se vio impactada, ¿ahora que debo hacer?

A pesar del posible impacto que se pueda tener de cara a los clientes y accionistas, las empresas deben preocuparse por reportar los fraudes o intentos de fraude en que se ven inmersas, de una manera homogénea, y acá un buen inicio es la lista de códigos de identificación de fraude promovida por el Centro Nacional de Fraude de los Estados Unidos.

Pienso que lo peor que una empresa financiera puede hacer, es reservarse que sufrió un fraude electrónico y buscar cómo solucionarlo; pues una empresa sola no puede hacer mucho contra los millones de malhechores electrónicos del mundo. Se hace necesario conglomerar el conocimiento en asociaciones, para combatir el crimen digital. Las empresas deben incorporse a este tipo de asociaciones para estar recibiendo y aportando constantemente, conocimiento sobre los nuevos tipos de ataques y las maneras de prevenirlos y contrarrestarlos.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

¿Cómo prevenir un impacto financiero fuerte?

Una de las principales acciones que una empresa debe tomar, es reconocer los factores de riesgo a los que está expuesta, así como tratar de buscar los avisos que se le presentan ya que pueden ser la antesala de un fraude.

Estos avisos o anomalías pueden ser clasificados en tres tipos: de comportamiento, estadísticos y organizacionales.

Las anomalías de comportamiento se presentan, cuando se determina un cambio en el estilo de vida de las personas, fuera de lo que estas pueden costear; las estadísticas se dan cuando los números no se ven bien, ya sean gastos, cuentas de tarjetas de crédito fuera de proporción y en general, cualquier cifra que salte de lo normal en los informes de una empresa; y las anomalías organizacionales se manifiestan cuando se ven esquemas de comunicación inadecuados dentro de la empresa, falta de transparencia o ausencia de controles.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Ante estos avisos hay algunos esquemas que se pueden utilizar para prevenir un impacto fuerte dentro de una empresa, entre ellos están:

- El uso de un gobierno corporativo efectivo.
    - Los gerentes deben saber exactamente la forma en que operan las empresas para que de esta manera, tengan plena conciencia de los riesgos de fraude a los cuales se están enfrentando.
    - Políticas de control de fraude
    - Se deben tener políticas claras y transparentes de cara a los fraudes y esquemas de mejoramiento continuo de ellas, para que se vayan adaptando a los esquemas cada vez más elaborados de fraude. Se deben establecer políticas específicas, en relación con la seguridad de la información: uso de correo electrónico, seguridad de los sistemas de autenticación, descarga de programas de Internet y uso de computadoras para propósitos personales.
- Monitoreo del personal
    - Para prevenir el fraude interno y el fraude en el cual un empleado colabora con un criminal, se debe tener esquemas de monitoreo del personal para garantizar que este es confiable; en especial, los empleados de muchos años que tienen un vasto conocimiento incluso de los esquemas de seguridad utilizados en la organización.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

- De la misma manera, los esquemas de monitoreo se deben extender a los consultores y contratistas con que se esté trabajando especialmente, con los que apoyan el montaje de los sistemas de monitoreo y seguridad.

Estos esquemas para prevenir un impacto fuerte pueden ser aplicados prácticamente a todo tipo de empresa, así como también otros marcos de trabajo reconocidos que ayudan a implementar de una manera correcta el concepto de gobierno de tecnología de información, el cual establece las pautas que se deben seguir para disminuir riesgos e implementar controles para prevenir y disminuir los impactos tanto de ataques internos como de ataques externos de diversos tipos. Existen también normativas que son aplicables de manera específica, a algunos tipos de empresa que contribuyen grandemente, a prevenir, detectar y mitigar los fraudes electrónicos y sus impactos.

Para las empresas emisoras y adquirentes de tarjetas de crédito, el norte a seguir es la adopción del PCI DSS ("*Payment Card Industry – Data Security Standard*" o Estándar de Seguridad de Información la industria de tarjetas de crédito), el que fue institucionalizado por las grandes marcas de tarjetas como VISA y MasterCard. Dicho estándar fundamenta seis objetivos principales, cada uno de los cuales se desglosa en requerimientos del estándar.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Objetivos	Requerimientos de PCI DSS
Construir y mantener redes seguras	1. Instalar y mantener configuraciones para proteger los datos del tarjetahabiente
	2. No utilizar configuraciones por defecto para contraseñas y otros parámetros de seguridad
Proteger datos del tarjetahabiente	3. Proteger los datos almacenados del tarjetahabiente
	4. Encriptar las transmisiones de datos del tarjetahabiente a través de redes públicas
Mantener un programa de gestión de vulnerabilidades	5. Utilizar y actualizar frecuentemente programas antivirus
	6. Desarrollar y mantener sistemas y aplicaciones seguras
Implementar medidas fuertes de control de acceso	7. Restringir el acceso a los datos del tarjetahabiente sólo al personal que necesita saberlos
	8. Asigner un código de identificación único a cada persona que accese la red
	9. Restringir el acceso físico a los datos del tarjetahabiente
Monitorear y probar regularmente las redes	10. Llevar control y monitorear todos los accesos a los recursos de la red y a los datos de los clientes
	11. Probar regularmente los sistemas y procesos de seguridad
Mantener una política de seguridad de la información	12. Mantener una política de seguridad de información para empleados y contratistas

Figura 3: Objetivos y requerimientos del estándar PCI DSS

Cabe mencionar que estas normativas no se deben tomar a la ligera, sino que es algo que debe ser permeado de una buena manera en la cultura organizacional para que esta se mantenga alerta todo el tiempo.

A manera de ejemplo, se presenta lo sucedido a principios del 2009 a la empresa Heartland Payment Systems, la cual fue certificada en el cumplimiento con PCI en agosto del 2008; y la que luego de esto, bajó la guardia y empezó a sufrir un fraude electrónico desde finales del 2008, el que fue anunciado públicamente en enero de 2009. Este evento es hoy en día clasificado como la fuga de información más grande de la historia, en la que más de 100 millones de registros de información de clientes se vieron comprometidos y el

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

impacto para la empresa, se puede observar de una manera muy clara en el precio de las acciones de la empresa.

Figure 4: Precio de las acciones de Heartland Payment Systems. Fuente:

www.moneycentral.com

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

En la figura 4 se muestra en el recuadro azul el impacto provocado, cuando se hizo público el fraude sufrido por la empresa, y los dos círculos rojos representan el punto más alto y más bajo del precio de la acción, en donde se puede ver que se pasó por una pérdida de valor de un 80% en aproximadamente 2 meses.

Con esto se muestra la importancia de mantenerse siempre alerta, para no sufrir un impacto fuerte; si a una empresa de esta importancia, certificada en el cumplimiento con PCI, le ocurrió este impacto financiero ¿cuál puede ser el impacto para una empresa como las que tenemos en Centroamérica?

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Conclusiones

El fraude es algo que no va a desaparecer, y aunque se esté poniendo mucho esfuerzo en conseguir que los sistemas sean cada día más seguros, se seguirán presentando fraudes cada vez más elaborados.

El reportar un fraude electrónico es en muchas ocasiones problemático y subestimado, dado el temor a verse públicamente expuesto; pero el no hacerlo, disfraza el impacto real que se está sufriendo en el ámbito mundial, debido a fraudes electrónicos; por tanto, este tipo de comportamientos no contribuye a erradicar este problema del mundo virtual, por lo que es imperativo, ser parte de la solución incorporándose a asociaciones que luchen contra estos fraudes y aportarles a estas, las vivencias propias para contribuir a erradicarlos.

Para reducir la cantidad de fraudes electrónicos en el mundo, se deben atacar los tres elementos que lo generan; por tanto, de alguna manera los gobiernos y grupos organizados para combatirlo deben buscar formas de reducir la motivación de los criminales, quizás a través de condenas más severas que los hagan pensar dos veces, antes de tratar de infringir la ley. Se deben aumentar los esfuerzos en la educación de las posibles víctimas, de manera que la cultura contra este tipo de crímenes inicie desde los usuarios finales y no solo desde los expertos en seguridad de información. Si se logra esta conciencia, la cantidad de víctimas y de fraudes disminuirá, apoyando esto a la desmotivación de los criminales en potencia. Por último, pero no menos importante, resulta continuar con los esfuerzos que se han venido haciendo por hacer las aplicaciones más seguras; al haber barreras más altas que enfrentar, también se está contribuyendo a disminuir la motivación de los villanos.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Una barrera relevante es la de tener un buen manejo de los riesgos que enfrenta una organización; para esto se necesita un correcto proceso de identificación y gestión de los riesgos, con lo que se debe determinar cuál es el apetito de riesgo que está dispuesto a aceptar una organización y gestionar los riesgos que superen dicho umbral.

Como se mencionó, existen marcos de trabajo que pueden apoyar en la gestión de riesgos de una empresa. Considero que es de suma importancia que los altos directivos de las organizaciones financieras empiecen a dirigir esfuerzos para la evaluación de las brechas que tienen, para la implementación de un esquema como el planteado por COBIT ("*Control Objectives for Information and related Technology*" - Objetivos de control para TI y tecnologías relacionadas), el cual provee una serie de métricas, procesos e indicadores que cooperan a implementar un efectivo gobierno de TI que ayude a maximizar los beneficios que dicha área aporta a la organización. En el caso específico de Costa Rica, este tema ya no es opcional, pues la Sugef ("Superintendencia General de Entidades Financieras") liberó en marzo de 2009 la ley 14-09, la cual exige la implementación de la mitad de los procesos que expone COBIT (17 procesos de 34). Este tipo de reglamentaciones deben ser vistas como un apoyo, más que como una ley que debe cumplirse; pues ayudará a que las entidades financieras se preparen de manera adecuada para enfrentar los constantes cambios del entorno y los persistentes riesgos, a que se enfrentan, ante ataques cada vez más elaborados.

Junto con la ley 14-09 vienen normativas encaminadas hacia el mismo objetivo de plantear mecanismos, para mitigar riesgos y proteger a la empresa de fugas de información. Los emisores y adquirentes de tarjetas de crédito deben mirar la normativa de PCI como un

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

norte que los puede guiar hacia un desempeño más adecuado de su trabajo, y que incluso les puede otorgar una ventaja competitiva al verse como entidades certificadas; pero acá es importante que las empresas miren esta normativa como algo en lo que tienen que estar en cumplimiento las 24 horas del día, los 365 días del año, y no solo en el momento de la certificación anual; pues basta solo un descuido para ser víctima de un fraude de proporciones como las mencionadas.

Lecturas interesantes a seguir, para ampliar sobre el tema de la implementación de un gobierno de TI con COBIT o PCI, para las empresas de tarjetas de crédito pueden ser las siguientes:

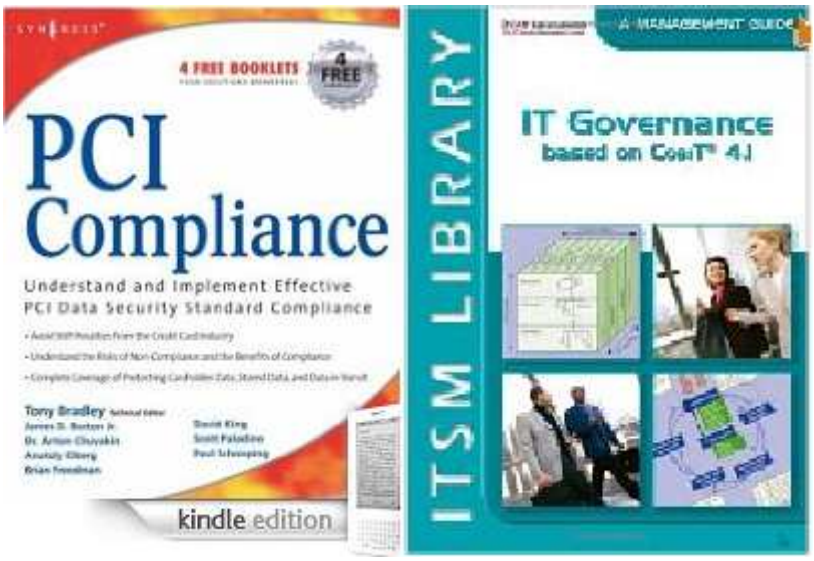

Figura 5: Lecturas posteriores sugeridas. Fuente: www.amazon.com

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

El nombre de los libros y la manera de encontrarlos es la siguiente:

PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance

http://www.amazon.com/PCI-Compliance-Understand-Implement-Effective/dp/B001OMKH2O/ref=sr_1_1?ie=UTF8&s=books&qid=1252292462&sr=8-1

IT Governance Based on Cobit 4.1: A Management Guide

http://www.amazon.com/Governance-based-Cobit-4-1-Management/dp/9087531168/ref=sr_1_1?ie=UTF8&s=books&qid=1252292638&sr=8-1

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Bibliografía

A Year of data breaches and losses. (Diciembre de 2008). *Credit Management.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Berner, R., & Carter, A. (21 de junio de 2005). *The Truth About Credit Card Fraud. Business Week Online.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Bernstein, C. (Abril de 2009). *The Cost of Data Breaches. Baseline.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Britt, P. (Junio de 2007). *Experts Tighten Securtity on Online Fraud. Information Today, 24(6), 41-41.* Recuperado el 19 de julio de 2009, de Academic Search Elite database.

Campbell, K., Gordon, L., Loeb, M., & Zhou, L. (Setiembre de 2003). *The economic cost of publicly announced information security breaches: empirical evidence from stock market. Journal of Computer Security, 11(3), 431.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (Otoño de 2004). *The Effect of Internet Security Breach Announcements on Market Valule: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce, 9(1), 69-104.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Costly Data Breaches Hurt Community Banks And Their Customers. (Setiembre de 2005). *Community Banker.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Data breaches cost FS firms 17% more than in other industries. (Marzo de 2009). *Banking Technology.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Data Breaches Skyrocket in 2008. (Marzo de 2009). *Information Management Journal.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

History, F. (s.f.). *Federal Bureau of Investigation*. Recuperado el 25 de julio de 2009, de Famous Cases, Willie Sutton: http://www.fbi.gov/libref/historic/famcases/sutton/sutton.htm

Identity Theft Center. (s.f.). Recuperado el 24 de agosto de 2009, de www.idtheftcenter.org

Kaper, S. (7 de febrero de 2007). *ACB: Breaches Cost Small Banks. American Banker, 172(26),20-20.* Recuperado el 19 de Julio de 2009, de Business Source Elite database.

Loeb, M. (Abril de 2004). *THE TRUE COST OF CYBERCRIME. Network Computing, 15(6), 69-69.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

MCQUEEN, M. (2 de febrero de 2009). *Data Breaches Cost Businesses More. Wall Street Journal - Eastern Edition, 253(26), B6.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Microsoft. (s.f.). *¿Qué son los virus, gusanos y troyanos?* Recuperado el 9 de agosto de 2009, de http://www.microsoft.com/latam/athome/security/viruses/virus101.mspx#EOD

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Oates, B. (Enero de 2001). *Cyber Crime: How Technology Makes It Easy and What to Do About It. Information Systems Security, 9(6),45.* Recuperado el 19 de julio de 2009, de Academic Search Elite database.

Ponemon Says Breaches Growing Costlier. (12 de febrero de 2009). *American Banker*. Recuperado el 19 de julio de 2009, de Business Source Elite database.

Rodier, M. (Enero de 2008). *Cost of Data Breaches Growing. Wall Street & Technology, 26(1), 10-10.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Rodier, M. (Marzo de 2008). *Cost of Data Breaches Increasing. Insurance & Technology, 33(3),32-32.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Sherstobitoff, R. (Setiembre de 2008). *Anatomy of a Data Breach. Information Security Journal: A Global Perspective, 17(5/6),247-252.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Vijayan, J. (6 de agosto de 2007). *Breaches Pushing Retailers to Adopt PCI. Computerworld, 41(32), 10-10.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Vijayan, J. (9 de febrero de 2009). *Data Breaches Continue to Get More Costly. Computerworld, 43(6),6-6.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com

Vijayan, J., & Weiss, T. (26 de junio de 2006). *List of Data Breaches Grows. Computerworld, 40(26),6-6.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Vioilino, B. (Marzo de 2009). *AS THE ECONOMY SINKS, DATA BREACHES RISE. CFO, 25(3), 25-29.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Wolfe, D. (23 de octubre de 2006). *Higher Costs for Data Breaches - Both Old and New. American Banker, 171(203), 22-22.* Recuperado el 19 de julio de 2009, de Business Source Elite database.

Bachiller en Informática. Candidato a Maestría en Administración de Empresas, ULACIT. Correo Electrónico: jorge.betancourth@gmail.com