¿Qué hacer si su negocio es víctima de robo de datos o ha tenido violaciones de seguridad?

Introducción

El objetivo de la siguiente información es ayudarlo a decidir cómo estar preparado y algunas medidas que debe tomar ante una eventual falla de seguridad respecto a ciertos tipos de datos e información. Como no es posible cubrir todos los escenarios y circunstancias, pueden existir otras consideraciones o medidas que usted podría seguir que no están incluidas en este revisión.

Reporte de Amenazas Mandiant's 2014 – cita que toma un promedio de 243 días para descubrir una falla. Dada la certeza de que alguna forma de ataque o falla de seguridad sucederá en su organización muy probablemente a través de dispositivos móviles, tiene mucho sentido considerar diferentes escenarios y planificar antes de que los incidentes ocurran. Un plan de seguridad establece pasos clave y también involucra personal clave.

Para la asistencia de un mejor entendimiento de sus obligaciones y para la adaptación de un plan de reacción ante una falla tecnológica para su compañía es altamente recomendable que consulte con su de departamento de tecnología y/o socios legales.

Conozca la Ley

Michigan ha promulgado leyes que requieren ciertas acciones sean tomadas y que los individuos sean notificados cuando una falla de seguridad compromete información personal. Si usted cree que su seguridad ha sido comprometida, usted debe revisar y entender cualquier obligación que puede tener bajo la ley **Mich. Comp. Laws §§ 445.63, 445.72.**

En adición a las leyes estatales descritas en la parte superior, leyes federales **(federal law)** podrían requerir notificaciones para ciertos tipos de violaciones de datos.

Instituciones Financieras están sujetas a la federal Gramm-Leach-Bliley Act (15 U.S.C. §§6801-6810) deben adoptar procedimientos para salvaguardar los datos de los clientes y notificar a los clientes cuando ha existido acceso no autorizado a sus datos, si la institución financiera determina que los datos han sido o probablemente mal usados. Directrices sobre cuando clientes de una institución financiera deberán ser notificados acerca de una falla de seguridad son publicados aquí FDIC.

Violaciones de datos personales que involucran **información médica u otra información de salud relacionada** también pueden incitar el requerimiento de notificar a ciertas partes. La ley

Pequeño Negocio, Gran Amenaza

HIPAA de notificación de violaciones, 45 CFR §§ 164.400-414, HIPAA requiere que todas la entidades y sus asociados de negocios provean notificaciones una vez que la violación de la información de saludo ha sucedido. La provisión de notificaciones similares y obligatorias por el Federal Trade Commission (FTC), aplica a proveedores de registro personales de salud y también a proveedores que actúan como terceros, de conformidad a la sección 13407 de la ley HITECH. Es muy importante recordar aunque no sea un proveedor medico en sí mismo. Estas leyes le aplican si su compañía trabaja de cerca con cualquier asociación que es un proveedor de servicios de salud u cualquier otra organización relacionada.

Para mayor información acerca de violaciones de seguridad haga click aquí HHS about HIPAA .

La ley HITECH también requeridas por la Federal Trade Commission (FTC) requiere se adopten leyes ante fallos que se aplican a proveedores de redes de basadas en información electrónica de salud así como también proveedores de servicios. Revise las leyes de notificación aquí FTC's breach notification.

Se ha convertido en "**buena práctica**", y no muy común para compañías, instituciones educativas y agencias de gobiernos de notificar a sus clientes y empleados en cuanto se ha experimentado o no un fallo de seguridad se requiere que sean notificados. Un ejemplo es cuando los nombres y correos electrónicos de los clientes han sido comprometidos. Aunque la exposición de estos fallos no produzcan robo financiero de identidad si han sido obtenido por criminales, muchas compañías han optado por notificar a sus clientes de todas maneras.

Antes de que una violación de seguridad ocurra

Primeramente y primordialmente si no dispone de lo siguiente: un plan y una respuesta de equipo definido, trabaje en ellos ahora mismo. Entendiendo su responsabilidad y planificando de antemano le asistirá gratamente en el evento de un fallo de seguridad. Las siguientes directrices le ayudaran a considerar todo lo que su plan debe contener:

Primero conozca su información.

- ¿Dónde está? (*"en la nube digital" vs. en un servidor en su compañía*).
- ¿Cómo fluye (*solamente en su oficina físicamente vs. dondequiera su equipo de ventas tiene acceso a través de dispositivos móviles).*
- ¿Quién tiene acceso a la información? (*todos tienen igual acceso o el acceso está basado en cada posición individualmente?*).
- ¿Su información esta encriptada – en tránsito y/o archivada?
- ¿Toda la información es considerada sensible o solamente secciones especificas?

Segundo, ¿Cómo su información está siendo monitoreada?

- Existe una bitácora que registra cada una de las personas que acceden al sistema (o intentan acceder) de información sensible? Investigadores de violaciones de seguridad recomiendan que todos los negocios implementen un sistema de seguridad de información y también un programa de monitoreo para asistir a descubrir actividades maliciosas y mitigar posibles ataques, asistir con acciones legales o proveer detalles/forenses a la compañía de seguros si es necesario hacer un reclamo.

Pequeño Negocio, Gran Amenaza

Tercero, comprensión de la información.

- ¿Porque es valiosa?
- ¿Quien desea robarla? Esto le ayudara a entender que tipo de atacantes pueden estar interesados en cometer una violación de seguridad de su sistema. Una sugerencia es contactar los organismos legales y ver si otras compañías han tenido el mismo tipo de violaciones de seguridad. Si este es el caso, trate de aprender todo lo que sea posible acerca del fallo.
    - ¿Que fue robado?
    - ¿Cuando el fallo de seguridad fue descubierto?
- Preguntas frecuentes – porque, como, cuando, donde, quien, para que pueda aprender de la experiencia desafortunada de la compañía y puede prepararse anticipadamente.

Personas a involucrar

- Conozca a quien puede llamar para solicitar ayuda
- Establezca un equipo de respuestas a incidentes
- Provea entrenamiento regular para empleados; preservando un equipo externo — incluyendo expertos forenses, consultores privados y firmas de comunicación —muy cercanas

Procedimiento a seguir

- Conozca qué tipo de información está protegiendo y donde está almacenada
- Ensaye hipotéticos escenarios de fallos de seguridad con su equipo de intervención
- Conozca cuales empleados tienen acceso a las diferentes aplicaciones y aprenda acerca de los reporte de obligaciones que existen en caso de un fallo.

Tecnología que necesita

- Establezca un sistema de registro de redes, y asegúrese que está suficientemente detallado
- Servidores de reserva y asegúrese que las copias de seguridad están bajo su control
- Aplicación de sistemas de gestión de datos y destrucción de información antigua
- Implementación total encriptación de discos duros en ordenadores portátiles
- Implementación de medidas de seguridad, como estándares de contraseñas
- Implementación DLP para monitorear el perímetro
- Efectivo manejo de la integración de seguridad y adquisiciones

Durante un fallo de seguridad

Sobre todo evite el pánico. Un fallo de seguridad no necesariamente significa que sus clientes serán victimas de robo de identidad. Si es no probable que sus clientes sean comprometidos como resultado del fallo de seguridad, comunicación con ellos será esencial.

Pequeño Negocio, Gran Amenaza

Una vez que la violación de información ha sido descubierta como para de "respuesta al incidente" consulte el sistema de respaldo de su empresa y el plan de recuperación. Si las copias de respaldo no se hacen rutinariamente, información expirada puede resultar en pérdida total en un instante; por lo tanto es crítico tener copias de seguridad frecuentes de los datos de la empresa.

Si usted decide o necesita contactar a sus clientes asegúrese que ellos sepan que su empresa se encargara de ellos. Evite acusaciones mutuas y atribución de culpas. Deje saber a sus clientes que su empresa trata el fallo de seguridad seriamente y que se está reaccionando ante la misma. Cumpla con las promesas realizadas. Cumpliendo sus obligaciones es esencial para no perder la confianza de sus clientes.

La siguiente información le ayudara a identificar vías para reducir el riesgo y exposición con respecto al robo de identidad.

Personas a involucrar

- Es importante mantener grupo pequeño de personas "que tienen el conocimiento"
- Contrate expertos forenses, un equipo de comunicaciones y un consejo privado desde el inicio
- Efectivamente maneje la respuesta a incidentes (project management)
- Anticipe amenazas internas y externas
- Considere impacto de terceras personas

Procesos a seguir

- Actué inmediatamente para remediar vulnerabilidades
- No se dirija al público rápidamente
- Lance una amplia red de extracción de datos
- Documente todas las acciones tomadas para que luego sean compartidas con reguladores
- Actualice su equipo de investigación
- No comunique números preliminares
- Considere el impacto de cada encuentro hallado en el negocio

Tecnología que necesita

- Tome secciones de memoria en tiempo real antes que apague los servidores
- Insista en imágenes forenses completas de los servidores y ordenadores portátiles
- Remueva los accesos a la red inmediatamente e incremente los registros de red
- Remueva copias de seguridad antiguas que están disponibles.
- Restablezca contraseñas rápidamente
- Tenga mucho cuidado manejando las evidencias

Tenga en mente, que existe un incremento en ransomware (acceso restringido a la información a cambio de un rescate monetario* ataques por hackers También es importante notar el compromiso de ***Personally Identifiable Information**** (PII) puede resultar en

litigaciones civiles en contra de su firma por el fiscal general del estado así como también otras acciones legales.

**Ransomware* – *un tipo de malware que previene o limita el acceso de los usuarios al sistema. Este tipo de malware obliga a las víctimas a pagar un rescate a través de métodos de pago en línea para permitirle acceder al sistema o tener la información de vuelta. Algunos ransomware encriptan archivos (llamados Cryptolocker).*

**Personally Identifiable Information (PII)* – *cualquier información que potencialmente puede identificar específicamente a un individuo. Esta información puede ser usad para distinguir una persona de otra y puede usarse para desautorizar anónimamente información. En otras palabras, esta información puede ser usada como propia o con otra información para identificar, contactar, o localizar una persona específicamente en contexto. PII incluye Números de Seguridad Social, números de licencia de conducir, información médica y cualquier otra información que se considere "publica".*

Después de un fallo

No asuma que se ha terminado hasta que se haya terminado. Asegúrese que el fallo y cualquier otro riesgo asociado han sido mitigados.

1er Paso: Revise sus obligaciones Legales y Éticas

Violaciones de seguridad son complejas; usualmente involucran un numero de leyes federales y estatales, las misma que dictan como y cuando notificar a clientes afectados, oficiales del estado (Fiscal General, Comisionados, reguladores), etc. Se sugiere que todos los negocios revisen y comprendan que se espera de su negocio – preferiblemente con el consejo de un abogado que es un experto en leyes de fallos de seguridad, ya que estas leyes y/o regulaciones pueden imponer estrictos plazos para el reporte de un fallo de seguridad. Al mismo tiempo el cumplimiento de obligaciones éticas con los clientes de su negocio, proveedores y empleados pueden requerir que se exceda la ley al pie de la letra.

2do Paso: No entre en pánico…y no se acelere en su respuesta

Una fuente de recursos confiable es el Ponemon Institute, y esta organización sugiere que los negocios deben actuar lo más pronto posible en respuesta a una violación de seguridad y notificar a los clientes. SIN EMBARGO, no se acelere en reunirse con los medios de comunicación hasta que haya sido autorizado por las fuerzas de la ley. Otra importante razón para NO acelerarse a compartir la información acerca del fallo de seguridad es que "compañías que responden rápidamente" actualmente terminan pagando más por el fallo, que compañías que esperaron un poco para ejecutar su respuesta estratégica y compilar todos los hechos posibles. La línea de fondo es un ciclo vicioso: Compañías terminan invirtiendo mucho tiempo corrigiendo el impacto de su misma mal información acerca de las acciones requeridas en casos de violaciones de seguridad así como hacen resolviendo el impacto del fallo original.

Pequeño Negocio, Gran Amenaza

3er Paso: Ejecute un Análisis, y Actué con los Resultados

Aunque ha sido comprobado que las violaciones de seguridad típicamente involucran fracasos al aplicar tecnología apropiadamente, los negocios deben crear y ejecutar iniciativas de cyber seguridad para dispositivos móviles, software, hardware, y firmware usando lo mejor de sus habilidades; aquí es donde la utilización de los servicios de un profesional provee un valor significativo.

Un problema que es imposible prevenir es la "pérdida o robo de ordenadores portátiles" problema que se debe tener en cuenta que sucederá en algún momento. Pero si su negocio impone estrictos requerimientos de encriptación en esos sistemas y requiere que empleados almacenen información sensible en su propia red en lugar del ordenador portátil, y el acceso es únicamente a través de conexiones VPN Redes Virtuales Privadas (*Virtual Private Network*)* . Los negocios también pueden combinar estas herramientas tecnológicas con políticas y entrenamiento de medidas que mantiene empleados responsables por la violación de políticas de seguridad de la información.

***virtual private network** – *un método de encriptación empleado para proveer remoto acceso seguro a una computadora sobre el internet. Habilita a los usuarios a enviar y recibir datos sobre redes públicas compartidas, como si los dispositivos estuvieran directamente conectados a la red privada, y estos se benefician de la funcionalidad, seguridad y manejo de las políticas de la red privada.*

Un análisis de los fallos de seguridad puede resultar en adicionales maneras de mejorar su negocio en el "uso de tecnología". La seguridad de la red y puntos finales, herramientas anti-malware, herramientas anti-phishing y políticas y otras soluciones pueden trabajar conjuntamente para proteger su empresa, a sus empleados, sus clientes y proveedores.

Otra sugerencia es contratar un consultor externo para que realice una auditoría de seguridad posterior al fallo de seguridad de los sistemas de la compañía y el manejo de procedimientos de la información. Usted debe pensar en que conoce el porqué del fallo de seguridad, por lo que un análisis externo objetivo puede brindarle un conjunto de respuestas muy diferente a tan vital pregunta.

4to Paso: Mantenga a sus Clientes y Empleados informados

La tecnología puede jugar un papel vital en ayudarle a su compañía a evitar futuras violaciones de seguridad. La información respecto a nuevas políticas y procedimientos pueden ser compartidas con empleados y clientes, pero no inunda s su audiencia con detalles técnicos acerca de los procedimientos de seguridad — es inútil (y peligroso) como se indica.

Personas a involucrar

- Use la exposición al fallo para promover la mejora del programa de seguridad a su junta
- Revisite la estructura de gobierno de la información, incluyendo seguridad, la parte legal y el manejo de riesgos

Pequeño Negocio, Gran Amenaza

- Entregue a sus empleados y clientes un mensaje transparente y consistente
- Use esta oportunidad para implementar entrenamiento en privacidad

Procesos a seguir

- Use esta oportunidad para expandir privacidad y programas de seguridad
- Documente las lecciones aprendidas
- No exagere con la comunicación o revisión de números
- Anticipe escrutinio a largo plazo
- Use esta oportunidad para implementar privacidad nuevas iniciativas para seguridad
- Construya un playbook

Tecnología que necesita

- Desarrolle un plan de remediación con mejoras tecnológicas
- Pruebe acciones de remediación
- Considere amplias mejoras en la compañía
- Preserve la evidencia de la investigación
- Actualice encriptación, medios externos, USB y políticas de correo electrónico
- Revise la nube digital y la preparación de terceros proveedores de tecnología

Fallos específicos en dispositivos móviles

(Incluyendo textos fraudulentos y otros problemas)

- Cada proveedor de servicios inalámbricos tiene un número y un correo electrónico para reportar fraudes, y donde se deben reenviar le el contenido de la información fraudulenta. Revise con su proveedor de servicios para asegurarse que los tiene en su archivo. Si recibe un texto de mensaje que sospecha es fraudulento o existe un riesgo de seguridad en alguna forma – NO LO ABRA – Inmediatamente reenvíelo al número de texto provisto por su proveedor. Haga los mismo si tiene sospecha de un correo electrónico; otra vez – NO LO ABRA – en su lugar, inmediatamente reenvié el correo electrónico sospechoso a la dirección electrónica provista por su proveedor para reportar fraudes
- Si sospecha que una aplicación descargada contiene virus, malware o es malicioso en alguna manera, notifique al proveedor de la aplicación y tenga a un profesional técnico en seguridad evaluando el impacto en su dispositivo móvil.

Fallo de un vehículo conectado

- No se alarme. Calmadamente de un paso atrás y evalué la situación antes de tomar cualquier acción. Asegúrese que puede explicar claramente la situación a personas necesarias como: oficiales de seguridad, el fabricante, el proveedor o el almacén de reparación.
- Si parece que su vehículo ha sido hackeado o manipulado, no maneje el vehículo hasta que haya sido evaluado y los problemas hayan sido resueltos.
- Si cree que existe un problema con el sistema de su vehículo conectado y parece que ha

sido hackeado, verifique con el fabricante para determinar si existe un problema por lo cual el retiro del vehículo ha sido iniciado de antemano y no necesariamente se trata de un problema de hackeo.

- Tan pronto sea posible actualice el sistema de su vehículo con el último lanzamiento de software y en el futuro implemente las actualizaciones oportunamente.

Resumen ante fallas de seguridad – Que hacer y Que no hacer

Qué hacer –

- ✓ Tenga un plan escrito listo para responder a fallas de seguridad
- ✓ Pruebe su plan antes de que la falla ocurra
- ✓ Identifique la respuesta en equipo a la falla de seguridad, asegúrese que las personas conocen que rol juegan cuando una falla sucede
- ✓ Tenga un plan de comunicación respecto a las fallas de seguridad.
- ✓ Conozca las regulaciones, estatutos, contratos que cubren sus obligaciones posteriores fallas de seguridad.
- ✓ Cuando una falla sucede, emplee todos los medios para prevenir mayor exposición de datos.
- ✓ Averigüe lo más pronto posible que sucedió y conserve la evidencia
- ✓ Contacte su compañía de seguros y busque asesoría legal respecto a si la falla genera requerimientos y si estos requerimientos se aplican a su compañía
- ✓ Involucre su departamento de tecnología y expertos legales si es necesario
- ✓ Tenga un borrador de modelo de comunicaciones listo a ser modificado dependiendo de los hechos.
- ✓ Contacte las fuerzas policiales, agencias de crédito y mantenga a los reguladores informados donde sea requerido por ley y donde sea apropiado.

Qué no hacer –

- × Retraso en proveer comunicaciones cuando el consejo legal determina que ellos son requeridos o es prudente que los tiempo de plazo sean estrictos
- × Comunicación con el público acerca de las fallas de seguridad hasta que conozca los hechos fundamentales.
- × Ignorar sus clientes y socios importantes – manteniéndolos informados
- × Acceder necesariamente a todas las demandas de los clientes de su negocio y socios – sopese las demandas cuidadosamente ante al plan de respuesta total
- × Escatimar en proveer ayuda a los consumidores – su buena voluntad podría acarrear Dificultades legales.
- × Olvidarse de actualizar su plan de respuesta posterior a las fallas de seguridad regularmente.

Pequeño Negocio, Gran Amenaza

NOTA IMPORTANTE:

El propósito de la siguiente información es ayudarle a decidir cómo puede empezar a preparar su negocio en contra de ataques cyber y algunas de las medidas que puede tomar en la eventual violación de seguridad con respecto a ciertos tipos de datos e información. Como no es posible cubrir todos los escenarios y circunstancias, existen otras consideraciones o medidas que su empresa necesitara seguir que no están incluidas en este documento. Para asistencia en una mejor compresión de sus obligaciones y la elaboración adaptada de un plan de reacción en contra de un fallo de los sistemas para su compañía, es altamente recomendable que consulte con su departamento de tecnología y/o socios legales.