Las 5 razones por las que debería contratar un seguro contra ciberataques

La amenaza que representa los riesgos cibernéticos ahora es tan tangible como las amenazas físicas a los activos de una empresa y se enfrenta cada vez más a la información electrónica, ya sea en los dispositivos móviles, ordenadores, servidores o en línea. Los riesgos cibernéticos están evolucionando y siendo cada vez más complejos, como la tecnología y la sofisticación de los criminales, lo que incrementa la probabilidad de una violación de datos en sus sistemas informáticos. Una vez que se produce una violación de seguridad, potencialmente hay una amplia gama de consecuencias adversas para una empresa.

El seguro cubre las consecuencias obvias y menos obvias de los riesgos cibernéticos.

1 ¿QUE DATOS TENGO?

- En la era digital las empresas son responsables de grandes cantidades de datos, tanto de sus clientes, como de sus empleados. A nivel individual, si los pagos se realizan con tarjeta de crédito o débito, usted es el responsable de esta información, así como de los datos de contacto de clientes, incluyendo nombres, direcciones y números de teléfono.
- Los comercios retail deben cumplir con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS) o estará sujeto a multas y sanciones impuestas por la Industria de Tarjetas de Pago (PCI).
- Los clientes proporcionan información más detallada al registrarse en programas de fidelización o emailing, así como la compra de pedidos online.
- Los datos de empleados son cada vez más sensibles, incluyendo detalles sobre la nómina y antecedentes clínicos.
- A nivel corporativo, el tratamiento de los datos es el mismo, en relación con los plazos de notificación.
- Si los datos no son íntegros, y posteriormente modificados, ya sea deliberadamente o no, esto podría tener repercusiones importantes para su negocio.
- Una violacion de seguridad con el consiguente robo de información al respecto de nuevas ubicaciones de tiendas, las estrategias de ventas o promociones, por mencionar algunas, respresentaría un coste muy elevado y dificil de cuantificar.
- La legiscion obliga a notificar por escrito la infracción a los terceros afectados.
- CyberEdge cubre los gastos de notificación y la póliza responde ante la legislación local del territorio o país.

2 EL COSTE TOTAL DE UNA BRECHA DE SEGURIDAD

Su empresa puede estar expuesta a los siguientes gastos:

- Multas regulatorias, incluyendo Tarjeta de Pago (PCI).
- Daños y perjuicios relacionados con reclamaciones de defensa ante terceros
- Diagnóstico de la fuente de la brecha o la pérdida de datos
- Reconfiguración de redes, restablecimiento de la seguridad y la restauración de datos y sistemas
- Gastos de notificación
- Monitorización de los archivos de crédito
- Implantación del plan de recuperación ante desastres

Una póliza de responsabilidad civil profesional no pagará una indemnización por incumplimiento de la legislación de protección de datos o el coste para la compañía de la brecha de seguridad.

3 CRISIS REPUTACIONAL

Las noticias de fugas de datos se propagan rápidamente, especialmente la comunicación en los medios sociales.
La confianza pública de su empresa puede disminuir en cuestión de horas.
La situación necesita una gestión cuidadosa tanto con los medios de comunicación como con clientes, empleados y accionistas.
Se requieren acciones rápidas y una respuesta de Comunicació y Relaciones Publicas para recuperar la confianza y proteger la reputación de la empresa.

CyberEdge proporciona un servicio de respuesta a incidentes cibernéticos.
Verizon, como expertos en provisión de soluciones de seguridad, responderá a incidencias cibernéticas ante ataques hacker y ofrecerá asistencia después de una violación de seguridad, asisténdole para la restauracion de los sistemas y servidores.

Deloitte Abogados ofrecerá la notificación y control de identidad.

La consultara Porter Novelli son expertos en restitución de la imagen de la sociedad y personas responsables.

4 ¿PODRÍA SU EMPRESA CONTINUAR CON EL NEGOCIO SIN SUS SISTEMAS DE TI ?

Si sus sistemas informáticos fallan, o experimentan una intrusión o fueran hackeados,

¿Cúal sería el efecto en su negocio?
¿Incapacidad para realizar transacciones comerciales y prestar el servicio requerido a los clientes?
¿Dañar las relaciones existentes con sus proveedores y obstaculizar el desarrollo de nuevo negocio?
¿La falta de stock?
¿La publicidad negativa?
Todo ello conduce a una pérdida de ingresos que está fuera de su control.
CyberEdge puede ayudar a cubrir la pérdida de ingresos, recuperar los datos perdidos y notificar a los afectados de la de la fuga seguridad

5 CONSECUENCIAS LEGALES/ NOTIFICACIÓN A LOS AFECTADOS

El robo de datos de tarjetas de crédito se ha incrementado notablemente y puede afectar a cualquier comercio que acepta transacciones mediante este sistema de pago. Usted tiene la obligación de cumplir con todas las leyes en materia de pago en dinero electrónico para prevenir el robo de identidad de sus clientes y la obligación legal en algunas jurisdicciones de notificar cualquier violación en la seguridad de datos, lo que supone unos gastos de notificación elevados a todos los afectados, además de incrementarse la probabilidad de recibir multas y/o sanciones administrativas del regulador local y reclamaciones de terceros.