VALUATIVE SAS NIT 830.121.091-0 Oficinas a nivel Nacional
info@valuative.co - www.valuative.co

EL CYBER SEGURO LOS RIEGOS CIBERNETICOS

UN ENFOQUE PARA SUSCRIPCION Y ATENCION DE RECLAMO CRITERIOS Y CONCEPTOS

PARTICULARIDADES DEL RIESGO CIBERNETICO

1

VALUATIVE
LIDERES EN INVESTIGACIÓN Y PROTECCIÓN PATRIMONIAL

Cra. 7 No.156 - 10 Of.1607 /Torre Krystal
Centro Empresarial North Point
Bogotá D.C., Colombia
PBX.: +57(1) 390 2846
info@valuative.co

VALUATIVE
LÍDERES EN INVESTIGACIÓN Y PROTECCIÓN PATRIMONIAL

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

EL CYBER SEGURO
LOS RIEGOS CIBERNETICOS

UN ENFOQUE PARA SUSCRIPCION Y ATENCION DE RECLAMO
CRITERIOS Y CONCEPTOS
PARTE 1
PARTICULARIDADES DEL RIESGO CIBERNETICO.

INTRODUCCION

Es común que la Empresas utilicen sistemas electrónicos para enviar, recibir o almacenar datos electrónicos. Dichos datos pueden incluir proyecciones de ventas, registros de impuestos y otra información propiedad de su empresa. Si los datos se pierden, son robados o dañados debido a una brecha de seguridad, podría ser muy costoso reemplazarlos o restaurarlos.

Dichos sistemas informáticos también pueden contener datos confidenciales que pertenecen a otras partes, como clientes, **empleados o proveedores**. Si los datos se pierden o son comprometidos por un pirata informático, los propietarios pueden demandar a su empresa por daños. Su empresa también podría incurrir en gastos de notificación sustanciales. Prácticamente, los estados tienen leyes que requieren que las empresas informen a las personas cuya información personal se ha visto comprometida en una **violación de datos**. Puede proteger su negocio contra los costos asociados con las violaciones de datos comprando una póliza de responsabilidad cibernética.

En éste contexto, se requiere tener claras definiciones de sobre las vinculaciones contractuales desde el punto de vista de los operadores de un cliente asegurado particular, por ello se hace necesario el definir con la mayor exactitud posible los términos *"Empleados o Proveedores"* y *"Violación de datos"*.

DEFINICIONES

¿Empleado o Contratista Independiente?

¿En qué se diferencia un empleado de un contratista independiente? Esta pregunta es importante si el asegurado emplea trabajadores. Como la mayoría de los empleadores, probablemente la ley le exija que proporcione **beneficios de compensación laboral** a los empleados lesionados en el trabajo. Sin embargo, no está obligado a proporcionar beneficios a los contratistas independientes lesionados.

Distinguir a los empleados de los contratistas independientes no es fácil. Por un lado, no existen pautas universales que los empleadores puedan utilizar para hacer esta distinción. Las reglas han sido establecidas por el Ministerio de Trabajo, por la DIAN y finalmente por el sistema legal a través de tribunales de

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

trabajo. Desafortunadamente, estas reglas no son consistentes. Por lo tanto, un trabajador considerado contratista independiente según un conjunto de reglas puede calificar como empleado según otro.

Significado de contratista independiente

El significado de contratista independiente varía de un contratante a otro. Algunos tienen estatutos específicos que definen el término. Otros se basan en la jurisprudencia (decisiones judiciales anteriores). Otros determinan el estado de un trabajador según una lista de criterios. Para calificar como contratista independiente, un trabajador debe cumplir con algunos o todos los criterios. En ocasiones, se designan a ciertos trabajadores, como, por ejemplo, los agentes de bienes raíces, como contratistas independientes en función de sus ocupaciones (para solo mencionar uno).

Un consenso unificado sobre lo que constituye un contratista independiente, muchas organizaciones aplican principios comunes. Uno de ellos tiene que ver con la independencia. Para calificar como contratista independiente, un trabajador, no el empleador, debe tener control sobre su trabajo.

En muchas Empresas, el proceso para determinar si un trabajador es un contratista independiente o un empleado comienza con las siguientes preguntas:

¿El empleador controla solo el resultado del trabajo? ¿El empleador también controla los medios y métodos por los que se realiza el trabajo? Si el trabajador es un contratista independiente, él o ella establecen el horario de trabajo y decide qué herramientas y procedimientos se utilizan para realizar el trabajo. El empleador controla únicamente el producto final.

¿El trabajador opera un negocio independiente que está separado del negocio del empleador? Un contratista independiente tiene un negocio establecido distinto del negocio del empleador. Él o ella realizan trabajos para empresas distintas del empleador.

Estos son solo algunos de los factores que los estados pueden considerar para determinar si un trabajador califica como contratista independiente. En consecuencia, tienen una gran relevancia al momento de evaluar la probabilidad de otorgar una cobertura de Cyber Seguridad y, por supuesto, del alcance de sus amparos, dependiendo de la actividad principal del contratante y de la manera de vincular a un contratista, que potencialmente pueda verse afectado por ataques cibernéticos, o incluso, resulte copartícipe de los mismos.

Por lo tanto, gran parte de la operatividad de un Cyber Seguro depende de la manera en que se vincula un colaborador a una empresa asegurada, y para efectos prácticos, la evaluación del riesgo cibernético dependerá de factores múltiples, entre los cuales se encuentra la forma de operar la información, por ejemplo, desde el punto de vista de Software e incluso del Hardware utilizado, pues las exposiciones varían cuando el Contratista tiene acceso solo a programas empresariales (controlados internamente) a cuando éste puede "manipular el mismo" según sus propias conveniencias. De igual forma ocurre con el Software, aunque realmente la probabilidad de iniciar un **Cyber Crime** a partir de un control parcial o total de los programas es mucho más difícil de que acaezca.

Auditorías de las Aseguradoras

Resultan fundamentales los controles guiados directamente desde el Mercado Asegurador al otorgar coberturas de **Cyber Crime** para dilucidar la exposición a riesgos cibernéticos. Por ejemplo, la auditoría asegura que se haya cumplido con las regulaciones exactas establecidas en la ley, desestimulando la probabilidad de cometimiento de fraudes por parte de éste tipo de trabajadores. Y éste es solo un elemento de riesgo de exposición a pérdida...

EL SEGURO DE RESPONSABILIDAD CIBERNETICA – COBERTURA POR FILTRACION DE DATOS – [Protección contra violaciones de Datos y Redes]

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

En 2017, hubo **1,579** violaciones de datos en los EE. UU. Según un informe publicado por el Centro de recursos de robo de identidad y CyberScout. Esto representó un aumento del 44,7% sobre el número de infracciones registradas en 2016. Una infracción de datos u otro tipo de **ataque cibernético** puede afectar seriamente a su negocio. Puede dañar sus datos, generar demandas contra su empresa y dañar la reputación de su empresa. Puede proteger el negocio contra muchos de los efectos de los delitos *cibernéticos* comprando *un seguro de responsabilidad civil cibernética.*

¿Necesita el solicitante (La Empresa u Organización) el seguro?

La cobertura de responsabilidad cibernética puede beneficiar a cualquier empresa que utilice datos electrónicos en sus operaciones diarias. Es posible que necesite esta cobertura si realiza alguna de las siguientes acciones:

- Comunicación con los clientes por correo electrónico, mensajes de texto o redes sociales
- Envíe o reciba documentos electrónicamente
- Anuncio de la empresa a través de medios electrónicos, como un sitio web o redes sociales
- Almacenamiento de datos de la empresa, como proyecciones de ventas, registros contables, documentos fiscales y secretos comerciales en una red informática
- Almacenamiento de información de identificación personal (PII, por sus siglas en inglés) sobre empleados, clientes, pacientes o prospectos en una red informática. Ejemplos de PII son nombres, números telefónicos personales y direcciones, números de tarjetas de crédito, fechas de nacimiento y números de seguro social.
- Venta de productos o servicios o proporcionar información a los clientes a través de sitio(s) web de empresariales.

Si bien estas actividades pueden permitir que su empresa funcione de manera eficiente, generan riesgos. Los datos que se almacena en un **sistema informático** podrían violarse, lo que resultaría en demandas contra su empresa. Los datos también podrían dañarse debido a un virus, un ataque de piratas informáticos u otra causa. Restaurar o reparar los datos puede resultar muy costoso.

PELIGROS DE LOS CYBER ATAQUES

Los ataques pueden originarse dentro o fuera de la Empresa

Podría pensarse que las pequeños empresas son objetivos poco probables para los ciber delincuentes, pero, lamentablemente, este no es el caso. Cada año miles de pequeñas empresas son víctimas de **phishing, malware, piratería** y otros tipos de ciberataques.

Los ciberataques contra las grandes empresas son bien publicitados por los medios de comunicación, mientras que los ataques contra las pequeñas empresas generan poca atención. Esto puede dar a las pequeñas empresas una falsa sensación de seguridad. Sin embargo, las empresas pequeñas son generalmente más vulnerables que las grandes porque tienen menos recursos para dedicar a la **seguridad**.

Los ataques son un riesgo grave

Los ciberataques son un riesgo grave para las pequeñas empresas. Esto fue confirmado por una **encuesta de ciberseguridad** que el **Ponemon Institute realizó** en 2018. La encuesta involucró a 1.045 pequeñas y medianas empresas en los EE. UU. y el Reino Unido. Aquí hay algunos hallazgos clave:

- El sesenta y siete por ciento de los encuestados sufrió un ciberataque en 2018 (en comparación con el 61% del año anterior).
- El sesenta por ciento de los encuestados que tuvieron una **violación de datos** dijeron que la causa fue un **empleado negligente** o un **contratista independiente**.
- Una gran mayoría de los encuestados experimentó un **exploit** o **malware** que eludió la detección de intrusos o el software antivirus de su empresa.

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

- Los **dispositivos móviles eran los puntos de entrada más vulnerables** a las redes informáticas de las empresas.

Tipos de ataques

Los tipos más comunes de ataques cibernéticos contra empresas, según **Cisco**, son **malware**, **phishing**, **ataques de denegación de servicio**, **ataques de intermediario**, **inyecciones de SQL** y **exploits de día cero**. En un ataque "**man-in-the-middle**", un criminal se interpone entre dos partes que realizan una transacción para poder robar datos. Una **inyección de SQL** implica un código malicioso que se instala en un servidor SQL (un tipo de software de administración de bases de datos desarrollado por Microsoft). Un **exploit de día cero** es un ataque que ocurre entre el momento en que se publica una vulnerabilidad y una solución está disponible.

Los ataques pueden provenir de dentro o fuera de su empresa. Los ataques internos a menudo son perpetrados por empleados sin escrúpulos. Los delincuentes ubicados en casi cualquier parte del mundo pueden cometer ataques externos. Algunos pueden ser perpetrados por **espías corporativos**.

Formas en que los espías corporativos "vigilan un negocio"

El espionaje corporativo no es nada nuevo y no se limita a la tecnología. Por ejemplo, en la década de 1800, East India Co. de Gran Bretaña robó secretos, plantas de té y semillas de China para pasar a dominar la industria del té. En 1997, un empleado de Gillette robó un nuevo diseño de maquinilla de afeitar y lo envió a un grupo de los principales competidores de Gillette; terminó yendo a la cárcel durante 27 meses.

Incluso los gigantes como Google no son inmunes. En 2010, Google escribió una publicación en un blog que hablaba de un sofisticado ciberataque que se originó en China un mes antes y terminó con la desaparición de un montón de **propiedad intelectual** de Google.

¿Qué aspecto tiene el espionaje corporativo?

El espionaje corporativo se ve glamoroso en las películas de espías, pero generalmente no es muy glamoroso en absoluto. Sin embargo, incluso si el espionaje corporativo es tan aburrido como una puntilla de puerta, aún puede causar grandes daños a una empresa.

Una cosa que no es el espionaje corporativo son las actividades legales de **investigación** de la **competencia**. Un competidor que revisa los registros públicos de una empresa es un juego completamente limpio al 100 por ciento.

Tipos de espionaje industrial

El espionaje corporativo industrial generalmente implica robo. Esto puede incluir el robo de recetas, técnicas, fórmulas químicas, información patentada y propiedad intelectual. Por lo general, esto implica que las personas son contratadas detrás de escena y roban secretos, ya sea para obtener ganancias financieras o para regresar a la empresa que percibieron que les ha perjudicado.

Ocasionalmente, el espionaje corporativo implicará robos reales. A veces esto se hace en persona, pero más a menudo son ellos los que piratean. Un tipo más nuevo de espionaje industrial es el uso de **malware** para bloquear a las personas de sus sistemas informáticos.

Protección contra los espías corporativos

Sugerencias que ayudan a una empresa a mantenerse segura:

Buen trato a los empleados y cuidado con a quienes se contrata. Una de las fuentes del espionaje corporativo son los empleados descontentos, que roban secretos comerciales y luego los difunden porque, simplemente, están enojados.

Por ello es fundamental tener una cultura empresarial en la que los empleados "estén contentos". También es importante tener cuidado a quién contrata para cualquier puesto. Al contratar a

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

las personas adecuadas para el trabajo, terminará con menos posibilidades de que un empleado descontento intente derribarlo con ellos.

Utilice contraseñas seguras y doble verificación siempre que sea posible. Las contraseñas pueden resultar abrumadoras. Y debido a esto, mucha gente usa la misma contraseña para todo. Esto es increíblemente peligroso. Lo deja expuesto a piratería y software malicioso.

En su lugar, utilice una herramienta de software de gestión de contraseñas. Estas herramientas, como **LastPass**, permiten establecer contraseñas complicadas para cada uno de los sitios, pero solo tiene que recordar una única contraseña. Esto realmente ayuda a aumentar la seguridad.

Además, donde sea posible, especialmente en sistemas críticos, debería utilizarse la doble autenticación.

Stripe [Empresa de procesamiento de pagos en Línea para negocios en Internet] es un ejemplo de una empresa que utiliza doble autenticación. Cuando inicie sesión en su sistema para ver sus pagos, le enviarán un código a su teléfono que deberá ingresar antes de que pueda ver algo. Esto le da una capa adicional de protección.

Y finalmente,

Debe Asegurarse el controlar la actividad de los empleados. Debido a que los empleados realizan una gran cantidad de espionaje corporativo, monitorear la actividad de los empleados es crucial. Puede rastrear fácilmente la actividad de los empleados en todos los sistemas digitales a través de un software simple. Hay muchos paquetes de software en el mercado que hacen esto. Y la clave para que esto funcione es ser transparente sobre lo que está haciendo.

A nadie le gusta que lo espíen, pero los empleados esperan ser monitoreados. Por lo tanto, es menester asegurar la divulgación sobre el seguimiento.

Cra. 7 No. 156 – 10 Of. 1607 / Edificio Torre Krystal
Bogotá D.C., Colombia
Pbx: +57 (1) 3902846
info@valuative.co

Casi cualquier empresa puede ser víctima de espionaje corporativo. Puede ser en forma de un ciberataque desde afuera, pero lo más probable es que sea una amenaza que provenga de su propia empresa. Tomar medidas para evitar el robo de secretos comerciales es importante para su éxito.

Fuente consultada: The Balance Small Business

Juan Carlos Lancheros Rueda
Cert CILA, BC's Mech Eng, BC's B.A, M.I.A, P.M.S, F.M.S.
C.E.O.