

Chubb Cyber

CHUBB®

Póliza para la gestión de
riesgos cibernéticos

Riesgos Cibernéticos



En el conectado entorno de hoy en día, la seguridad cibernética se ha convertido en una preocupación común. Sin embargo, los analistas temen que en muchos sectores industriales, algunas de las empresas no sean conscientes de su responsabilidad. Frecuentemente, las empresas no entienden los riesgos de privacidad de datos y cibernéticos en su organización hasta que sucede una situación de este tipo.

Cualquier empresa podría verse afectada por incumplimiento relacionado con el manejo de la información sensible de sus clientes o empleados. Incluso, el extravío de un equipo portátil, si no se gestiona adecuadamente, puede convertirse en un desastre en las relaciones públicas de la empresa, destruyendo no sólo la marca, sino también sus finanzas.

Los riesgos cibernéticos por su impacto y prevalencia han sido mencionados dentro del reporte presentado este año por el Foro Económico Mundial (WEF) "The Global Risk Report 2018": "los ataques en contra de empresas casi se han duplicado en cinco años y los incidentes que antes se consideraban algo fuera de lo común se están volviendo más y más comunes.

La afectación causada por el ataque Wannacry afectó 300 mil computadoras en 150 países y NonPetya causó pérdidas trimestrales de 300 millones de dólares para varias empresas afectadas".

En Latinoamérica, según la firma ESET, en su reporte de ESET Security Report Latinoamérica 2018 destaca que "el 45% de los participantes afirmó haber sufrido un incidente de seguridad relacionado con algún tipo de malware, lo que significa que al menos tres de cada cinco empresas en la región sufrió por lo menos un incidente de seguridad".

Como líder mundial en seguros cibernéticos, Chubb entiende el negocio de la protección. A través de nuestra experiencia y capacidades en todo el mundo, junto con la experiencia en Latinoamérica en seguros y gestión de riesgos, trabajamos para ayudar a las empresas en su crecimiento de manera confiable.

Chubb Cyber

Una solución completa en riesgos.



Más de 15 años de experiencia en riesgos cibernéticos

Nuestro equipo Global dedicado a los riesgos cibernéticos, cuenta con una experiencia de más de 15 años en suscripción y siniestros.

En Chubb sabemos que los riesgos cibernéticos no respetan fronteras y pueden atacar desde cualquier lugar y en cualquier momento a cualquier organización con consecuencias globales.

Con esta experiencia internacional, estamos preparados para entender y responder a los retos actuales y futuros en riesgos cibernéticos de nuestros clientes.

Pasando de los seguros a la gestión de riesgos empresariales

Nuestros suscriptores y especialistas en riesgos, apoyan a nuestros clientes ayudándoles a identificar y prevenir las posibles situaciones que pudieran ocasionar incidentes cibernéticos.

Estamos orgullosos de ayudar a convertir el mercado de seguros de una simple póliza, a una solución integral de control de pérdidas y gestión de riesgos.

Actualmente, los siguientes aspectos de riesgo tecnológico crean preocupación en los expertos en riesgos:

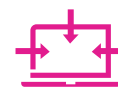
30%
Fallas del sistema



29%
Amenazas de los avances tecnológicos en el modelo de negocio existente



33%
Hackeo/Ataques de denegación de servicio





La mejor oferta del mercado

- Equipo de atención a siniestros disponible 24/7, brindando atención ante cualquier situación de riesgo cibernético
- Asistencia de proveedores que proporcionan una avanzada administración de riesgos durante la vigencia de la póliza
- **Sencillez de la póliza y estructura de soluciones integrales con el respaldo de un asegurador global de clasificaciones de solidez financiera AA de Standard & Poor's y A++ de A.M. Best.**



La respuesta al incidente es fundamental

En Chubb sabemos que cuando se trata de un evento cibernético, las primeras horas son cruciales por lo que en alianza con proveedores especializados, contamos con la disponibilidad de un gerente dedicado a la atención de incidentes; una de las características importantes de Chubb.

Con disponibilidad los 365 días del año, las 24 horas al día, un experto evalúa la situación, atiende las necesidades urgentes y toma las medidas apropiadas en el momento indicado, incluso cuando se requiera de la atención de expertos en cualquier lugar del mundo. Todo dependiendo de las circunstancias y enfocado en las necesidades del cliente.

Qué Esperar: El Proceso.

Antes de que ocurra un incidente...

Los Asegurados de Chubb Cyber pueden descargar la aplicación Chubb Cyber Alert o visitar la página: www.chubbcyberalert.com/enrollment/enroll.php para inscribirse. La inscripción permite reportar con un solo clic cuando ocurre un incidente.

Cuando ocurre un incidente...



Chubb Cyber



Escenarios

Considere los siguientes escenarios con base en experiencias actuales de siniestros y pregúntese si cuenta con un seguro adecuado:



Violación al Gobierno Corporativo de parte de los empleados

Causa de la acción:

Negligencia y violaciones que derive en la interrupción de operaciones

Detonante de la cobertura:

Interrupción del negocio, responsabilidad por privacidad, costos de recuperación, gastos por reparación de daño

Tipo de empresa: Comercio

Número de empleados: 20

Ingreso anual: \$5 millones USD

Descripción de la situación:

Un empleado de una tienda de equipo de cómputo ignoró las políticas y procedimientos internos y abrió un aparentemente inofensivo archivo dentro de un email. Al día siguiente, los sistemas de pedidos y las cajas registradoras comenzaron a fallar y el sistema estaba deficiente a consecuencia de fallas en la red.

Resultado:

La tienda de equipo de cómputo incurrió en \$100,000 USD en gastos de investigación y recuperación. También se incrementaron los gastos de operación en \$20,000 USD y se perdieron ingresos por \$50,000 USD derivado de las operaciones deficientes.

Gastos totales asociados al evento:
\$170,000 USD

Un empleado con acceso al sitio de Recursos Humanos, vende información personal de empleados

Causa de la acción:

Negligencia y responsabilidad por privacidad

Detonante de la cobertura:

Gastos por reparación del daño y pérdida de datos

Tipo de empresa:

Firma de servicios profesionales

Número de empleados: 25

Ingreso anual: \$7.5 millones USD

Descripción de la situación:

Un empleado deshonesto accedió a la plataforma de Recursos Humanos de un proveedor de servicios profesionales. El empleado extrajo información y la vendió al mercado negro antes de ser aprehendido. Por consiguiente, varios casos de robo de identidad fueron realizados en contra de empleados de la firma.

Resultado:

El proveedor de servicios profesionales contrató un investigador forense y un consultor de cumplimiento externo. También comunicó a los empleados sobre la violación, estableció un call center y proporcionó monitoreo y reparación del daño a los empleados afectados.

Costo total: \$75,000 USD



Escenarios



Invasión de la privacidad a consecuencia de robo de laptop

Causa de la acción:

Negligencia por robo de laptop que llevó a la invasión de la privacidad

Detonante de la cobertura:

Gastos por reparación del daño, responsabilidad por privacidad, interrupción del negocio, costos de recuperación, multas, extravío de tarjetas

Tipo de empresa: Empresa de Energía

Número de empleados: 100

Ingreso anual: \$20 millones USD

Descripción de la situación:

La laptop de un ejecutivo de una empresa de energía fue robada de un auto de la empresa. La laptop contenía información importante de clientes y empleados. A pesar de que el archivo estaba encriptado, la contraseña de acceso al equipo era sencilla y el NIP del archivo estaba comprometido.

Resultado:

Después de evaluar la naturaleza de la información de la laptop con un experto en investigación forense y un consejero de cumplimiento externo con un costo de \$50,000 USD, la compañía decidió voluntariamente notificar a los clientes importantes y empleados. También instaló un call center, monitoreo y restablecimiento

de servicios. Los costos extras ascendieron a \$100,000 USD y la compañía incurrió en gastos por \$75,000 USD correspondientes a la investigación regulatoria en varios estados. Finalmente, la compañía fue multada con \$100,000 USD por apartarse de su política de privacidad de datos.

Costo total: \$325,000 USD

Extorsión cibernética, interrupción del negocio y gastos extras a consecuencia de robo de información

Causa de la acción:

Violación del contrato y negligencia

Detonante de la cobertura:

Extorsión cibernética, gastos por reparación del daño, responsabilidad por privacidad, interrupción del negocio, costos de recuperación

Tipo de empresa: Firma de abogados

Número de empleados: 55

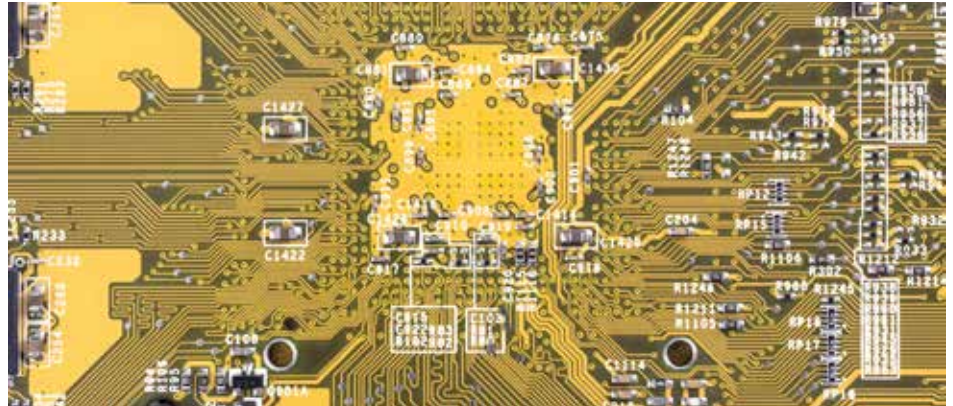
Ingreso anual: \$20 millones USD

Descripción de la situación:

Una organización desconocida vulneró la red de una firma de abogados y obtuvo acceso a la información sensible de los clientes, incluyendo la propuesta de adquisición de una compañía pública de tecnología, el prospecto de un inversionista y una considerable lista de acciones legales



Escenarios



con información personal identificable de los demandantes. Un investigador forense de tecnología determinó que un malware fue instalado en la red. Poco tiempo después recibieron una llamada del delincuente pidiendo 10 millones USD para no subir la información a internet.

Resultado:

La firma de abogados incurrió en gastos por \$2 millones USD por la investigación, negociación, pago del rescate por extorsión cibernética, notificaciones, monitoreo de créditos y robo de identidad, servicios de recuperación y honorarios de consultores independientes. Igualmente tuvo pérdidas por \$600,000 USD debido a la interrupción del negocio y gastos adicionales asociados a la desconexión del sistema.

Costo total: \$2.6 millones USD

Un fabricante paga por invasión a la privacidad perpetrada por un intermediario

Causa de la acción:

Un intermediario roba información personal derivando en negligencia e invasión a la privacidad

Detonante de la cobertura:

Gastos por reparación del daño, pérdida de datos y responsabilidad por privacidad

Tipo de empresa: Fabricante

Número de empleados: 50

Ingreso anual: \$10 millones USD

Descripción de la situación:

Un fabricante arrendó una copiadora por dos años. Durante ese periodo la compañía realizó copias de información personal identificable propiedad de clientes y empleados, incluyendo números de cuentas de pensión, número de licencia de conducir y otra información que facilitaba la identificación personal. Al finalizar el plazo de arrendamiento el fabricante devolvió la copiadora al arrendador a través de un intermediario. Previo a la devolución de la copiadora, un empleado deshonesto del intermediario, accedió a la información de la copiadora con fines maliciosos.

Resultado:

El fabricante incurrió en gastos por \$75,000 USD para la contratación de una investigación forense, notificaciones, monitoreo de la identidad, reparación del daño y honorarios de un consultor independiente. También incurrió en gastos por \$100,000 USD en defensa legal.

Costo total: \$175,000 USD

Riesgos Cibernéticos



Definiciones

Los riesgos cibernéticos cada vez más forman parte del diálogo entre nuestros agentes y sus clientes, ofrecemos una guía corta con la terminología asociada con términos y definiciones de uso común con fines informativos. Para más información sobre este u otros temas, por favor contacte a su agente.

Ataque DoS (Denial of Service Attack): Tipo de ataque en un servidor que es diseñado para inundarlo de información sin valor.

Ataque DDos (Distributed Denial of Service): La información de entrada que inunda al network de la víctima se origina de diferentes fuentes, haciendo difícil la detección de usuarios/tráfico legítimos de los falsos y casi imposible de detener dado que el origen está en muchos puntos.

Ataque Waterhole: Ataque donde los usuarios son llevados a un sitio comprometedor en donde el atacante planta malware en los visitantes del sitio.

Botnet: Se refiere a una red de computadoras “robot” que automáticamente transmiten spam, malware, o virus sin el conocimiento del usuario. También son llamadas “zombies” dado que usualmente son inyectados por un troyano y controladas por el creador del botnet y no por el dueño de la computadora.

CERT (Equipo de respuesta a Emergencias de Computadora): Equipo de expertos que manejan incidentes de seguridad cibernética.

Cyber: Frefijo usado en numerosos términos que describen cualquier cosa relacionada con el internet. El ciberespacio es un terreno no físico creado por sistemas computacionales.

Hacker White Hat: Hacker que usa sus habilidades para exponer vulnerabilidades del sistema antes de que hackers maliciosos (conocidos como Black Hat Hackers) las exploten. Típicamente son contratados por las organizaciones para mejorar los sistemas de seguridad.

IDS (Sistema de Detección de Intrusión): Sistema pasivo de monitoreo diseñado para alertar sobre actividades sospechosas que pueden resultar en virus, worms (gusanos) o hackeo. IDS no es un firewall ya que unicamente señala alertas y no las previene o detiene.

IPS (Sistema de Prevención de Intrusión): Combinación de un IDS y una aplicación firewall para protección. El IPS es generalmente considerado como la próxima generación del IDS.

Inyección SQL (Lenguaje Estandar Query): Forma de ataque a un sitio con base de datos en donde el atacante “inyecta” comandos SQL no autorizados para atravesar firewalls. Esta es una forma muy común de intrusión en el crimen cibernético.

Malware: Abreviación de software malicioso, generalmente diseñado para acceder secretamente a un sistema sin el consentimiento del dueño y roba información con fines ilegales. Malware incluye virus, caballo de troya, crimeware, rootkits y worms (gusanos).

Metatags: Código oculto insertado en páginas web que permiten a los buscadores agrupar rápidamente la información de las páginas.

PCI DSS (Sistema de Seguridad de la Industria de Pago con Tarjeta, a veces denominado PCI): Estándar de seguridad de propiedad de información desarrollado por MasterCard, Visa, American Express, Discover y JCB International usado para asistir comercios en la prevención de fraudes con tarjeta y mejorar la seguridad en torno en



Definiciones

el procesamiento y almacenamiento de información de tarjetas. PCI direcciona los requerimientos mínimos de seguridad como firewalls, encriptamiento y antivirus.

Phishing: Una estafa y/o timo en internet que recopila información personal. Spear phishing está más dirigido a recolectar información de usuarios específicos o confidencial.

PII (Información Personal Identificable): Información única que establece una identidad individual.

PKI (Infraestructura de Llave Pública): Sistema de certificados digitales, autenticaciones y otras autoridades de registro que verifican y autentican la validez de cada parte involucrada en una transacción de Internet. PKIs están evolucionando y no hay un estándar para configurarlos.

Rootkits: Software malicioso que es activado cada vez que el sistema empieza a funcionar. Son difíciles de detectar porque son activados antes de que el sistema operativo ha empezado a funcionar por completo. Los Rootkits pueden interceptar información de terminales, conexiones a red y del teclado.

Servicios en la Nube: Un tipo de recursos de computación que se basan en compartir y usar recursos vía internet en lugar de servidores locales o equipos personales para manejar aplicaciones.

Software de aplicaciones (a veces llamados programas para end-user): Incluyen programas de bases de datos, procesadores de palabras, hojas de cálculo. Estas no se pueden usar si no se tiene un sistema operativo y utilidades de sistema.

Sniffer: Programa o equipo que monitorea el viaje de información en un servidor. Estos programas pueden ser usados tanto para fines legítimos e ilegítimos.

Troyano Caballo de Trojano: Programa destructivo que se distingue a él mismo como una aplicación benigna pero que está diseñada para destruir y borrar archivos. usualmente no son detectados por software antivirus.

Worms (Gusanos): Es un tipo especial de virus que se puede autoreplicar y usar memoria. Pero a diferencia de un virus, los worms (gusanos) no pueden atacar a otros programas.

Virus: Programa que es cargado en una computadora y que inicia sin el conocimiento del usuario. Todos los virus de computadoras son hechos por el hombre e incluso autoreplicables. Es peligroso porque rápidamente usan la memoria disponible y llevan al sistema a detenerse. Otros tipos más peligrosos de virus son capaces de transmitirse a ellos mismos a lo largo de redes sobrepasando los sistemas de seguridad.

Vulnerabilidades Día cero: Vulnerabilidad en un código fuente que es desconocida por el desarrollador cuando es tomado por hackers para lanzar un “ataque día cero”.

Acerca de Chubb



Chubb es la compañía de seguros de propiedad y daños que cotiza en bolsa más grande del mundo. Con operaciones en 54 países ofrece seguros comerciales y personales en daños y bienes, accidentes personales, seguros complementarios de salud, reaseguro y vida a un diverso grupo de clientes.

La compañía se distingue por un extenso portafolio de productos y servicios, capacidad global de distribución, una excepcional fortaleza financiera, excelencia en suscripción, gran habilidad en la gestión de reclamaciones y operaciones locales globalmente.

Las aseguradoras de Chubb atienden a corporaciones multinacionales, pequeñas y medianas empresas a las que ofrecen servicios y seguros de propiedad y daños; clientes patrimoniales y de alto valor que requieren de protección a sus apreciables bienes; personas que adquieren seguros de vida, accidentes personales, salud complementaria, hogar, auto y otras coberturas especializadas; compañías y grupos de afinidad que ofrecen o proveen programas de accidentes y salud y seguros de vida a sus empleados o miembros y a aseguradoras que administran el riesgo con coberturas de reaseguro.

LATAM

Sandra Cabrera
Regional Cyber Manager
+57 (1) 326-6200 x 1903
Sandra.Cabrera@Chubb.com

Argentina

Esther Garcia Tagliaferri
Financial Lines Manager
+54 (11) 4114-4040
Esther.GarciaTagliaferri@Chubb.com
chubb.com/ar

Brasil

Humberto Pita
Financial Lines Director
+55 (11) 4504-4354
Humberto.Pita@Chubb.com
chubb.com/br

Chile

Marcelo Barrios
Financial Lines Manager
+56 (2) 2549-8340
Marcelo.Barrios@Chubb.com
chubb.com/cl

Colombia

Ana Mateus
Financial Lines Manager
+57 (1) 326-6200 x 1111
Ana.Mateus@Chubb.com
chubb.com/co

Cyber.Latam@Chubb.com

Ecuador

Natalia Villagran
Financial Lines Manager
+59 (34) 370-0400 x 4164
Natalia.Villagran@Chubb.com
chubb.com/ec

México

Yadim Trujillo
Financial Lines Director
+52 (55) 5258-5800 x 7697
Yadim.Trujillo@Chubb.com
chubb.com/mx

Panamá

Monica Gomez
Casualty & Financial Lines UW
+(507) 380-2232
Monica.Gomez@Chubb.com
chubb.com/pa

Perú

Natalia Rosas
Financial Lines UW
+51 (1) 417-5027
natalia.rosas@chubb.com
chubb.com/pe

Puerto Rico

Rafael Sanchez
Financial Lines Manager
+1 (787) 274-4774
Rafael.Sanchez2@Chubb.com
chubb.com/pr

Chubb. Insured.SM

Para consultar la totalidad de los términos y condiciones por favor remitirse a la póliza de cada producto o consultar a Chubb Seguros. El material contenido de este folleto no está destinado a proporcionar asesoramiento legal o de otro tipo sobre cualquiera de los temas mencionados, sino que se presenta para información general solamente.