Lecciones del Apagón de CrowdStrike para tu empresa

En la actualidad existe infraestructura digital y tecnológica (propia o de terceros) de la que dependen prácticamente todas las empresas para operar, más allá de su tamaño, sector o giro. Esta dependencia de los sistemas digitales, si bien ha traído consigo innumerables beneficios en términos de eficiencia y alcance, también ha expuesto a las organizaciones a nuevos y complejos riesgos.

El reciente apagón informático experimentado por CrowdStrike, una de las empresas líderes en ciberseguridad, **nos sirve como un claro recordatorio de la vulnerabilidad inherente a nuestros sistemas digitales y la crucial importancia de implementar prácticas de resiliencia robustas.**

No hay escape a los riesgos de un mundo digital

El 19 de julio de 2024, CrowdStrike, conocida por proporcionar servicios de seguridad de endpoint, inteligencia ante amenazas y servicios de respuesta a incidentes, provocó una serie de fallos informáticos a nivel global, congelando la operación en diversas industrias. El impacto financiero de sus efectos aún no ha sido cuantificado, pero ya se le reconoce como el fallo cibernético más importante de la historia.

El incidente subraya una realidad ineludible: ninguna organización, por más sofisticada que sea su infraestructura de seguridad, está completamente a salvo de interrupciones, errores humanos o ataques.

En un mundo donde la digitalización se ha acelerado dramáticamente, amplificando las repercusiones de cada uno de los eslabones de la cadena (al final éste es un proveedor de otros sistemas operativos y no un producto de consumo masivo), la resiliencia digital es un imperativo estratégico para todas las organizaciones.

La resiliencia empresarial en el contexto digital va más allá de la mera recuperación tras un incidente. Se trata de la capacidad de una organización para anticipar, prepararse, responder y adaptarse a cambios incrementales y disrupciones repentinas, manteniendo la continuidad de las operaciones y salvaguardando a las personas, los activos y la reputación general.

La creciente sofisticación de las amenazas cibernéticas, junto con la expansión de la superficie de ataque debido a la adopción

de tecnologías como la nube, el Internet de las Cosas (IoT) y la Inteligencia Artificial (IA), han elevado el perfil de riesgo de las empresas. Los ciberataques o incidentes disruptivos ya no son una cuestión de "si" ocurrirán, sino de "cuándo".

Esta realidad exige un cambio de paradigma en la forma en que las organizaciones abordan la ciberseguridad y la resiliencia.

Un aspecto crucial de este nuevo paradigma es la adopción de un enfoque integral hacia la ciberseguridad, que implica no solo invertir en tecnologías de seguridad avanzadas, sino también en el diseño de planes de seguros robustos, en la formación del personal, la creación de una cultura de seguridad en toda la organización y el desarrollo de planes de continuidad de negocio efectivos. La resiliencia digital debe integrarse en todos los aspectos de las operaciones empresariales, desde la planificación estratégica hasta las operaciones diarias.

El elemento clave para una gestión integral de riesgo es la evaluación cualitativa y cuantitativa de los riesgos cibernéticos que nos permita diseñar soluciones de mitigación y de transferencia de riesgo a través de pólizas hechas a la medida de cada organización. Entendiendo que los riesgos cibernéticos evolucionan y se vuelven más complejos día con día, las pólizas de seguro deben ser adaptadas a la realidad, si bien, estos seguros nacieron con el objetivo de proteger reclamos de responsabilidad civil frente a brechas de seguridad o violación de la información confidencial, durante los últimos años han transformado su enfoque a proteger riesgos cibernéticos que no impliquen propiamente una responsabilidad, sino pérdidas propias por interrupción en la red, fallos de seguridad, extorción cibernética y accesos no autorizados. Sin embargo, frente al reciente incidente es evidente que otros riesgos cibernéticos latentes como un error humano, fallos del sistema y proveedores externos de servicios tecnológicos también deben ser considerados cunado se busca una cobertura.

Hoy en día existen póliza cibernéticas que de manera afirmativa buscan extender su cobertura a estos riesgos no intencionados o maliciosos, pero debe contarse con el acompañamiento de un bróker experto que analice los alcances de dichas coberturas dado a que aún existen muchas limitantes en las consecuencias que pueden ser cubiertas y que seguirán siendo un foco rojo para los aseguradores dado a que un riesgo sistémico como el de Crowdstrike puede causar afectaciones agregadas a nivel global y limitar cada vez más el apetito de cobertura si no se cuentan con medidas de ciberseguridad robustas.

Así mismo un punto **sumamente importante** ante incidentes no maliciosos, se recarga en las responsabilidades contractuales profesionales por parte de los proveedores de tecnología, por lo que las pólizas de errores y omisiones para estas empresas serán un factor clave, así como las cláusulas contractuales que se definan entre las organizaciones y estos proveedores.

Resiliencia digital

La inversión en resiliencia digital debe verse como una inversión estratégica en el futuro de la empresa, no como un mero gasto en TI. Las organizaciones resilientes son más capaces de adaptarse a las disrupciones, recuperarse rápidamente de los incidentes y, en última instancia, mantener la confianza de sus clientes y partes interesadas, así como la facilidad de tener un acceso confiable y de mayor apetito al mercado de seguros y reaseguros. En un mundo donde la reputación puede destruirse con un solo incidente cibernético, la resiliencia se convierte en un diferenciador competitivo clave.

El incidente de CrowdStrike también subraya la importancia de la preparación y los ejercicios regulares. Incluso las mejores defensas pueden fallar, y cuando lo hacen, la rapidez y eficacia de la respuesta pueden marcar la diferencia entre un incidente menor y una crisis mayor. Las organizaciones deben realizar regularmente simulacros de incidentes cibernéticos, involucrando no solo al equipo de TI, sino también a la alta dirección y a los equipos de comunicaciones y legales.

Otro aspecto crucial es la necesidad de una colaboración más estrecha entre las empresas, los proveedores de servicios de seguridad y las agencias gubernamentales. Las amenazas cibernéticas evolucionan rápidamente, y ninguna organización puede mantenerse al día por sí sola. El intercambio de información sobre amenazas, las mejores prácticas y las lecciones aprendidas son esenciales para construir un ecosistema digital más resiliente.

Para ayudar a las organizaciones a mejorar su postura de ciberseguridad y resiliencia, aquí están cinco recomendaciones de WTW para la gestión de ciberseguridad:

Adoptar un enfoque de seguridad en capas	Implementar múltiples capas de seguridad que incluyan firewalls, sistemas de detección y prevención de intrusiones, autenticación multifactor y cifrado de datos. Ninguna medida de seguridad es infalible, pero múltiples capas pueden dificultar significativamente el éxito de un ataque.
Fomentar una cultura de ciberseguridad	Educar y capacitar regularmente a todos los empleados sobre las mejores prácticas de seguridad cibernética. La seguridad es responsabilidad de todos, no solo del departamento de TI. Implementar políticas claras sobre el manejo de datos sensibles, el uso de dispositivos personales y la respuesta a posibles amenazas.

Desarrollar y probar planes de continuidad de negocio	Crear planes detallados para mantener las operaciones críticas en caso de un ciberataque u otra interrupción digital. Realizar simulacros regulares para asegurar que estos planes sean efectivos y que todo el personal esté familiarizado con sus roles y responsabilidades durante un incidente.
Mantener sistemas y software actualizados	Implementar un programa riguroso de gestión de parches para asegurar que todos los sistemas y software estén actualizados con las últimas correcciones de seguridad. Las vulnerabilidades no parcheadas son una de las principales vías de ataque para los ciberdelincuentes.
Blindar la operación con seguros cibernéticos	Que en el peor escenario posible, permiten la recuperación de costos, robustecen la resiliencia, aceleran la recuperación y dan acceso a expertos en ciberseguridad y gestión de crisis para responder de la mejor manera a los incidentes.

En conclusión, el incidente de CrowdStrike sirve como un poderoso recordatorio de que en el mundo digital actual, la resiliencia y la ciberseguridad son imperativos estratégicos para todas las organizaciones. A medida que la infraestructura empresarial se vuelve cada vez más digital, la inversión en estas áreas no es solo una medida defensiva, sino una fuente de ventaja competitiva. Las organizaciones que adopten un enfoque proactivo y holístico hacia la resiliencia digital estarán mejor posicionadas para navegar los desafíos del paisaje digital en constante evolución y prosperar en la economía del futuro.

Adicional lo invitamos a leer **nuestro informe de alerta** donde exploramos las implicaciones del incidente en cara a los seguros, ofreciendo una guía clara de como identificar la cobertura dentro de sus pólizas.

En WTW tenemos la experiencia y el conocimiento para otorgar el apoyo necesario en estos tiempos de crisis.

Alerta – Cliente
Corte global de CrowdStrike

La reciente interrupción tecnológica de CrowdStrike resalta la fragilidad de los sistemas informáticos a una escala global.

Organizaciones de todo el mundo, incluidas aerolíneas, bancos, telecomunicaciones, medios y la atención médica han estado lidiando con los impactos de una interrupción de la tecnología global atribuida a CrowdStrike, una empresa de ciberseguridad cuyo software es utilizado para protegerse contra hackers y violaciones externas.

Este informe explora las **implicaciones del seguro**, centrándose en el **fallo del sistema**, las pérdidas por interrupción de la actividad empresarial, así como la relevancia de coberturas y exclusiones que deben tenerse en consideración. Asegúrese de estar preparado conociendo la **respuesta de su póliza** a este tipo de incidentes y tomando medidas proactivas en la documentación de pérdidas y la notificación a las aseguradoras.

La noche del jueves 18 y la madrugada del viernes 19 de julio de 2024 el mundo ha sufrido un apagón tecnológico sin precedentes, que ha paralizado a muchos sectores empresariales. La interrupción fue el resultado de una actualización automática lanzada por CrowdStrike a su agente Falcon Windows, causando que los sistemas Windows entraran en un bucle de bloqueo con una constante Pantalla Azul de la Muerte (BSOD).

Pocas horas después comenzaron a aparecer en línea numerosos dominios nuevos, todos ellos con un tema común: el nombre de CrowdStrike a lo que la Agencia de Ciberseguridad de las Infraestructuras de Estados Unidos (CISA) aclaró que la interrupción no estaba relacionada con un ciberataque o alguna actividad maliciosa. Sin embargo, CISA señaló que «los actores de amenazas están aprovechando este incidente para phishing y otras actividades maliciosas.»

George Kurtz, CEO de CrowdStrike, aconsejó a los clientes afectados que se comunicaran con los representantes de CrowdStrike a través de los canales oficiales. En momentos de pánico, las personas son más susceptibles a las estafas, lo que las convierte en objetivos principales para los ciberdelincuentes. Aunque los ataques de phishing suelen aparecer después de acontecimientos importantes, la magnitud de los cortes del viernes ha creado un gran número de víctimas potenciales.

Es habitual que los ciberdelincuentes aprovechen situaciones caóticas para lanzar ciberataques, especialmente aquellos que pueden crearse y personalizarse rápidamente, como las campañas de phishing por correo electrónico o texto.

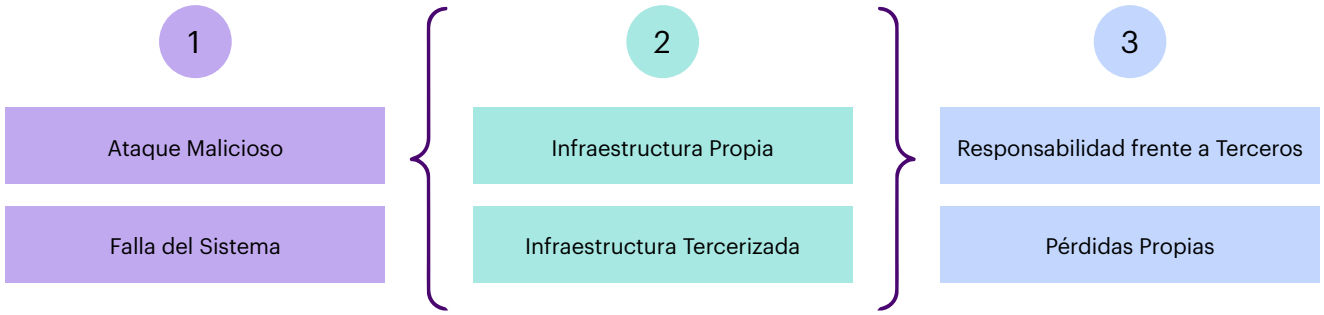
Implicaciones del Seguro Cibernético

Suponiendo que la comunicación de CrowdStrike, sobre esta interrupción es verídica y que no fue causada por un incidente de seguridad o un ataque cibernético, podemos tener una mirada al seguro cibernético, analizando algunos clausulados donde se exprese una definición afirmativa sobre **“fallo del sistema”** (definida comúnmente como un acto o fallo no intencional y no planificado de un sistema informático). Del mismo modo, el error humano podría estar dentro del alcance de esta definición como un error operativo o error de programación, cuando dichas definiciones se diferencian y distinguen contra un **“fallo de seguridad”** o **”acceso no autorizado”**, es más probable que el clausulado del seguro abarque dichos eventos dentro de alguna cobertura y debe validarse el alcance real de estas definiciones dentro de las coberturas y exclusiones de la póliza analizada.

1. ¿Cómo identificar la cobertura disponible dentro de mi póliza Cyber?

Originalmente las pólizas cibernéticas daban cobertura solamente para “ataques maliciosos” o “fallas de seguridad” en los sistemas propios del asegurado, sin embargo, hoy en día las pólizas han evolucionado en su lenguaje adaptándose a la realidad de las empresas quienes actualmente utilizan una compleja y dinámica **cadena de suministro de proveedores tecnológicos** para mantener sus procesos a la vanguardia como pueden ser; servicios de web-hosting, procesamiento de pagos, seguridad y gestión de datos, almacenamiento de datos, servicios de nube, Plataforma como Servicio (PaaS), Software como Servicio (SaaS), Infraestructura como Servicio (IaaS) o cualquier tipo similar de servicios informáticos o de Cómputo tercerizados.

En este sentido debemos desglosar las causas, afectaciones y consecuencias que puedan detonar una reclamación o daño dentro de una póliza de acuerdo con lo siguiente:



1. **Causa:** Primero debemos identificar la causa del evento, entender si fue un ataque malicioso o una falla del sistema, nos permitirá ubicar si estas definiciones se encuentran dentro de nuestra póliza y con ello determinar el alcance que pueden tener en las coberturas o exclusiones.

2. **Afectaciones:** Después es importante entender si la causa del evento se originó en nuestra infraestructura tecnológica o si proviene de una infraestructura tercerizada por nuestra cadena de suministro tecnológico, estas definiciones deberán mencionarse en la póliza para su fácil identificación, primordialmente la de nuestros sistemas y en adición las tecnologías de proveedores de servicios tecnológicos o que no sean propias.

3. **Consecuencia:** Finalmente, debemos tener clara la consecuencia del ataque, si este ha ocasionado una brecha de información que pueda conllevar responsabilidades frente a terceros o si esta solamente ha propiciado una interrupción de nuestro negocio generando pérdidas en nuestros activos digitales y en nuestra generación de ingresos, sin conllevar responsabilidades frente a terceros.

Una vez identificados los puntos anteriores, podemos inferir si se tiene la cobertura dentro de nuestra póliza, iniciando por un análisis a nivel de definiciones, posteriormente dentro del clausulado de coberturas y finalmente sobre las exclusiones expresas.

2. ¿Cuáles son las coberturas que pueden verse activadas ante esta situación?

En caso de identificar un lenguaje ampliado frente a proveedores de servicios de tecnología dentro de mi póliza, podemos identificar ciertas coberturas que pueden verse afectadas con diversos alcances.

Algunos clausulado tienen cobertura afirmativa expresa para proveedores externos de servicios (Contingent/Dependent), esta cobertura busca resarcir los efectos negativos del asegurado como consecuencia de un evento proveniente de su proveedor. La forma en la que funciona la cobertura depende del clausulado:

En algunas ocasiones se ofrece la cobertura, pero solo para la interrupción del negocio del asegurado (pago de lucro cesante y costos extra), derivada del evento que sufra el proveedor.

En algunos textos se ampara esta situación para errores y fallas del sistema (caso de Crowdstrike).

Y en otros casos solo se cubre el evento cuando ocurre un fallo de seguridad (ataques maliciosos).

En la mayoría de los textos, si hablamos de una situación interna de un proveedor de servicios tecnológicos, que no surja por un ataque malicioso, no se cubre, ya que esto se trata de un tema contractual entre el asegurado y su proveedor, por ende, el asegurado puede reclamarle directamente al proveedor.

En otras ocasiones no se trata de una cobertura como tal, si no, que se incluyen a los proveedores dentro de la definición de sistema de cómputo, en ese caso si la afectación es a los sistemas del asegurado, y/o a los sistemas de un proveedor externo, se podría activar cualquiera de las coberturas de la póliza.

En resumen, para que una póliza de riesgos cibernéticos cubra las pérdidas que se puedan ocasionar por un evento como el ocurrido a *Crowdstrike*, se debe contar con:

- Cobertura de proveedores (entre más general el tema de proveedores mejor).
- Que se active por fallas del sistema y/o errores humanos.
- Tener clara la consecuencia que estaría cubierta y hasta (responsabilidad frente a terceros o interrupción de la red) y analizar las exclusiones del seguro.

En conclusión, podemos decir que las pólizas deben ser analizadas en detalle para determinar su alcance de cobertura frente a riesgos no maliciosos y no controlados por el asegurado.

3. ¿Debo notificar a mi aseguradora?

Alentamos a cualquier cliente que se haya visto afectado por este evento o sospeche que pueda tener una afectación, que se comunique inmediatamente con su equipo de corretaje de WTW para analizar la notificación de la circunstancia o del posible incidente de acuerdo con los términos y condiciones de su póliza.

La notificación es un requisito umbral para activar la cobertura del seguro y deben investigarse y documentarse rápidamente.

4. ¿Qué medidas puedo tomar para protegerme ante estos eventos?

Para ayudar a las organizaciones a mejorar su postura de ciberseguridad y resiliencia, aquí están cinco recomendaciones de WTW para la gestión de ciberseguridad:

Adoptar un enfoque de seguridad en capas: Implementar múltiples capas de seguridad que incluyan firewalls, sistemas de detección y prevención de intrusiones, autenticación multi factor y cifrado de datos. Ninguna medida de seguridad es infalible, pero múltiples capas pueden dificultar significativamente el éxito de un ataque.

Fomentar una cultura de ciberseguridad: Educar y capacitar regularmente a todos los empleados sobre las mejores prácticas de seguridad cibernética. La seguridad es responsabilidad de todos, no solo del departamento de TI. Implementar políticas claras sobre el manejo de datos sensibles, el uso de dispositivos personales y la respuesta a posibles amenazas.

Desarrollar y probar planes de continuidad de negocio: Crear planes detallados para mantener las operaciones críticas en caso de un ciberataque u otra interrupción digital. Realizar simulacros regulares para asegurar que estos planes sean efectivos y que todo el personal esté familiarizado con sus roles y responsabilidades durante un incidente.

Mantener sistemas y software actualizados: Implementar un programa riguroso de gestión de parches para asegurar que todos los sistemas y software estén actualizados con las últimas correcciones de seguridad. Las vulnerabilidades no parcheadas son una de las principales vías de ataque para los ciberdelincuentes.

Blindar la operación con seguros cibernéticos: Que, en el peor escenario posible, permiten la recuperación de costos, robustecen la resiliencia, aceleran la recuperación y dan acceso a expertos en ciberseguridad y gestión de crisis para responder de la mejor manera a los incidentes.

¿Qué sigue?

Si bien el escenario vivido con Crowdstrike ya ha tenido antecedentes similares a menor escala como fueron los eventos de IFX y Solar Winds, es claro que la resiliencia empresarial va más allá de la recuperación tras un incidente. Se trata de la capacidad de anticipar, prepararse, responder y adaptarse a cambio y disrupciones repentinas, manteniendo la continuidad de las operaciones y salvaguardando a las personas, los activos y la reputación. Contar con seguros especializados es crítico e indispensable para tener protección financiera en caso de un incidente, pero también para obtener acceso a recursos y experiencia tanto para la prevención, como para respuesta a dichos incidentes.

En un mundo donde la reputación puede destruirse con un solo incidente cibernético, la resiliencia se convierte en un diferenciador competitivo clave.

Las organizaciones que adopten un enfoque proactivo y holístico hacia la resiliencia digital estarán mejor posicionadas para navegar los desafíos del paisaje digital en constante evolución y prosperar en la economía del futuro.

Comuníquese con nosotros para saber cómo podemos ayudarlo a adaptar su enfoque de gestión de riesgos cibernéticos y cobertura que se adapte a su perfil de riesgo y necesidades comerciales.

Contactos

Argentina
Rosario Ariztegui
Head of Finex
Directo: +54 911 57437298
rosario.ariztegui@wtwco.com

Brasil
Ana Albuquerque
Head of FINEX
Directo: +55 11 9 8854 4381
ana.albuquerque@wtwco.com

Colombia
Susana Andrade
Head of Finex
Directo: +57 313 6484802
susana.andrade@wtwco.com

Chile
Caroline Baes
Head of Finex
Directo: +569 5189 8623
caroline.baes@wtwco.com

Centro América
Ana Barreto
Head of Finex
Directo: +57 300 689 6250
ana.barreto@wtwco.com

México
Paola Carrillo
Head of Finex
Directo: +52 55 1384 0451
paola.carrillo@wtwco.com

Perú
Giafranco Tapia
Head of Finex
Directo: +51 949 224 358
gianfranco.tapia@wtwco.com

Venezuela
Claudia Patricelli
Head of FINEX
Directo: +58 212 2045279
claudia.patricelli@wtwco.com

LATAM
Rodrigo Flores
Head of Cyber LatAm
Directo: +52 55 4383 8517
rodrigo.flores@wtwco.com

LATAM
Marcela Visbal
Head of FINEX Product LatAm
Directo: +57 311 8044188
marcela.visbal@wtwco.com

LATAM
Maike Brückner
Head of FINEX Broking LatAm
Directo: +57 316 3998110
maike.bruckner@wtwco.com

Acerca de WTW
En WTW (NASDAQ: WTW), proporcionamos soluciones basadas en datos y basadas en perspectivas en las áreas de personas, riesgo y capital. Aprovechar la visión global y la experiencia local de nuestros colegas que prestan servicios en 140 países y mercados, lo ayudamos a agudizar su estrategia, mejorar la resiliencia organizacional, motivar a su fuerza laboral y maximizar el desempeño. Trabajando hombro a hombro con usted, descubrimos oportunidades para el éxito sostenible y proporcionar una perspectiva que lo motive. Obtenga más información en wtwco.com.

wtwco.com/social-media

WTW-julio de 2024