Deloitte.

CFO Insights
Siete costos ocultos de un ataque cibernético

Hay muchas maneras como un ataque cibernético puede afectar – y costar – a una organización, y los impactos variarán dependiendo de la naturaleza y severidad del evento.

Las percepciones comunes, sin embargo, principalmente están formadas por lo que las compañías están requeridas a reportar públicamente – principalmente robo de información personalmente identificable, datos de pagos, e información de la salud personal. Las discusiones tienden a centrarse en los costos relacionados con notificación del cliente, monitoreo del crédito, y la posibilidad de juicios legales o sanciones regulatorias. Y gracias al trabajo importante hecho en esta área, la industria generalmente está convergiendo en el cálculo del "costo por registro" por las violaciones de los datos del consumidor.[1]

Sin embargo, raramente considerados de manera completa son los casos de robo de propiedad intelectual [intellectual property (IP)], espionaje, destrucción de datos, ataques a las operaciones centrales, o intentos para desactivar la infraestructura crítica. Debajo de la superficie, esos ataques pueden tener un impacto mucho más importante en las organizaciones y conducir a costos adicionales que son tanto más difíciles de cuantificar como a menudo ocultos ante la vista del público. Un nuevo estudio de Deloitte, "Beneath the surface of a cyberattack: A deeper look at business impacts" [Debajo de la superficie de un ataque cibernético: Una mirada profunda a los impactos de negocio], recientemente esbozó la profundidad y la duración, en términos financieros, de los incidentes cibernéticos.[2] En esta edición de *CFO Insights*, nos centraremos en siete costos que típicamente no son aparentes y en por qué es importante incluirlos en el cálculo del costo total de un ataque cibernético.

Debajo de los costos de superficie
El general, el reporte cibernético identificó 14 impactos de negocio que tiene un incidente cibernético que se da durante el proceso de cinco años de respuesta al incidente – siete "por encima de la superficie" y siete costos "ocultos." Para los costos intangibles identificados, fueron usadas varias técnicas de modelación financiera para estimar el daño (vea el recuadro "Asignación de valor a las pérdidas intangibles"). Y en los escenarios presentados, los costos directos comúnmente asociados con las violaciones de datos de lejos fueron menos importantes que los costos ocultos. De hecho, en los escenarios de Deloitte, equivalieron a menos del 5% del impacto total del negocio.

Con el respaldo de

The CFO Program

Dado el impacto, los CFO deben ser conscientes de los siguientes siete costos ocultos:

1. **Las primas de seguros se incrementan.** Los incrementos de las primas de seguros son los costos adicionales que la entidad asegurada puede incurrir para comprar o renovar pólizas de seguro contra el riesgo cibernético luego de un incidente cibernético. Hay disponibles pocos datos públicos sobre los incrementos actuales de las primas luego de los ataques cibernéticos. Deloitte realizó investigación informal entre proveedores líderes de seguros cibernéticos y encontró que no es raro que el tomador de la póliza enfrente un incremento del 200% en las primas para la misma cobertura, o posiblemente incluso la negación de cobertura hasta que se satisfagan condiciones exigentes luego de un incidente cibernético. De acuerdo con las fuentes de Deloitte, los factores que influyen en los costos futuros incluyen: la voluntad y la profundidad de la información proporcionada por el tenedor de la póliza en la revisión del incidente; los planes del tomador de la póliza para mejorar el manejo del incidente u otros aspectos de su programa de seguridad; litigios anticipados; y supuestos relacionados con el nivel de "maduración" de la seguridad cibernética de la compañía.

2. **Costo incrementado para elevar la deuda.** El costo incrementado para elevar la deuda ocurre cuando, como resultado de una caída en la calificación del crédito, la organización víctima enfrenta tasas de interés más altas para el capital prestado, ya sea cuando eleva la deuda o cuando renegocia deuda existente. Las organizaciones parecen que son percibidas como prestamistas de riesgo más alto durante los meses siguientes a un incidente cibernético. Deloitte analizó la calificación del crédito de nueve compañías públicas (de la misma industria y comparables en tamaño) y observó un promedio de calificación del crédito A por parte de Estándar & Poor's, y valoró esas compañías contra compañías que recientemente habían sufrido un incidente cibernético. Observó que, en el corto plazo, las agencias calificadoras típicamente redujeron un nivel a las compañías que habían experimentado un incidente cibernético.

3. **Disrupción o destrucción operacional.** El impacto de la disrupción o destrucción operacional es una categoría de costo altamente variable que incluye las pérdidas debidas a manipulación o alteración de las operaciones normales de negocio y los costos asociados con reconstruir las capacidades operacionales. Esto podría incluir la necesidad de reparar equipo e instalaciones, construir infraestructura temporal, desviar recursos de una parte del negocio a otra, o incrementar recursos actuales para respaldar operaciones alternativas de negocio para reemplazar la función de los sistemas que temporalmente se hayan caído. También incluiría pérdidas asociadas con la incapacidad para entregar bienes o servicios. La naturaleza de la disrupción operacional – y por consiguiente el método apropiado de calcular su impacto – es muy específica para cada situación y requiere conocimiento directo de los distintos componentes de la información.

4. **Pérdida de valor de las relaciones con el cliente.** Durante el período inicial inmediatamente siguiente a la violación, puede ser difícil rastrear y cuantificar cómo se pierden muchos clientes. Los economistas y los equipos de mercadeo enfocan este desafío mediante asignar un "valor" a cada cliente o miembro para cuantificar qué tanto tiene que invertir el negocio para adquirir ese cliente o miembro. Luego miran los probables ingresos ordinarios que ese cliente o miembro generará para el negocio con el tiempo. Esos números pueden ser evaluados por industria y organización particular para estimar qué tanta inversión se necesita para atraer y adquirir nuevos clientes.

5. **Valor de la pérdida de ingresos ordinarios del contrato.** El valor de la pérdida de ingresos ordinarios del contrato incluye los ingresos ordinarios y la pérdida última de ingresos, así como también la pérdida de oportunidad futura asociados con contratos que sean terminados como resultado de un incidente cibernético. Para determinar el impacto financiera de la pérdida de contratos o primas, Deloitte estimó el valor de los contratos en casos de prueba tanto antes como después del ataque cibernético. Luego de un ataque cibernético. Si la compañía sujeto fuera a perder contratos, se asumió que habría una disminución en los ingresos ordinarios. Luego fue determinado el valor presente (significando el estimado del valor de la corriente futura de ingresos descritos en términos de dólares presente; recibir un dólar hoy vale más que recibir un dólar en el futuro, dado que uno podría ganar intereses en ese dólar) de los flujos de efectivo que la compañía ganaría durante el término de los contratos.

6. **Devaluación del nombre comercial.** La devaluación del nombre comercial es una categoría intangible de costo que se refiere a la pérdida en el valor de los nombres, marcas, o símbolos que una organización usa para distinguir sus productos y servicios. El nombre de la marca está asociado con el nombre de una compañía específica o con el nombre de un producto específico, mientras que el nombre comercial se relaciona con la organización en su conjunto. Para determinar el impacto financiero de un incidente cibernético en el nombre comercial de una compañía, tiene que ser evaluado el valor probable del nombre comercial tanto antes como después del incidente cibernético. Para valuar el nombre comercial mismo, Deloitte empleó el método de alivio-ante-la-regalía. El método del alivio-ante-la-regalía, comúnmente usado para valuar activos de IP tales como nombres comerciales, estima el valor mediante analizar lo que otra entidad tendría que pagar para licenciar el nombre comercial de la compañía.

El análisis de Deloitte involucró establecer un "honorario por regalías" razonable mediante mirar los honorarios o tarifas por regalías pagados en transacciones actuales de regalías por tipos similares de IP, y el análisis de los márgenes de utilidades a través de las industrias a las cuales pertenecen los casos de prueba, para determinar la capacidad de pago que tendría una compañía típica en la industria.

7. **Pérdida de propiedad intelectual.** La pérdida de IP es un costo intangible asociado con la pérdida del control exclusivo sobre secretos comerciales, derechos de copia, planes de inversión, y otra información de propietario y confidencial que pueda llevar a pérdida de ventaja competitiva, pérdida de ingresos ordinarios, y daño económico duradero y potencialmente irreparable para la compañía. Los tipos de IP incluyen, pero no están limitados a, patentes, diseños, derechos de copia, marcas comerciales, y secretos comerciales. A diferencia de otros tipos de IP, los secretos comerciales están protegidos de manera indefinida hasta tanto sean revelados públicamente. De manera similar al valor de un nombre comercial, el valor de la IP es estimado mediante aproximar qué tanto otra parte pagaría para licenciar esa IP.

Una imagen más completa del costo

Para todos quienes prestan atención a las violaciones importantes, los líderes de los negocios, incluyendo los CFO, raramente ven lo que ocurren detrás de los muros de la organización que se esfuerza por recuperarse de un ataque – hasta que les ocurre a ellos. Por consiguiente, si bien los incidentes cibernéticos pueden comenzar como un problema de tecnología, típicamente se extienden más allá del dominio de la tecnología y golpean el corazón del valor y el desempeño del negocio.

Entender los impactos menos obvios de un ataque cibernético requiere un enfoque multidisciplinario que integre el conocimiento profundo de los incidentes cibernéticos con el contexto del negocio, las técnicas de valuación, y la cuantificación financiera. Pero con mejor visibilidad en el rango amplio de los potenciales impactos de negocio – incluyendo los siete esbozados aquí – los líderes pueden transformar la manera como administran el riesgo cibernético y mejorar su capacidad para recuperarse cuando ocurra un ataque cibernético.

Asignación de valor a las pérdidas intangibles

En el reporte "*Beneath the surface of a cyberattack: A deeper look at business impacts*" [Debajo de la superficie de un ataque cibernético: Una mirada profunda a los impactos de negocio], fueron usadas varias técnicas de modelación para estimar el valor de la pérdida de IP, el daño al nombre comercial, y el impacto de la pérdida de relaciones y contratos con el cliente. Los siguientes conceptos son útiles para entender esos métodos.

La valuación y la cuantificación financiera están asociadas con un punto específico en el tiempo. Dados el valor del dinero en el tiempo y el rango amplio de factores internos y externos imprevistos que también pueden impactar el valor futuro de un activo, la intención del proceso de valuación es asignar un valor estimado o beneficio financiero a un activo en un punto específico en el tiempo – en este caso, el tiempo en el cual fue descubierto el ataque cibernético. El estudio aplicó el método ampliamente aceptado de los flujos de efectivo descontados según el enfoque de ingresos, que de manera amplia conlleva estimar el valor presente de los beneficios económicos proyectados a ser derivados del uso del activo.

Método con-y-sin. El método "con-y-sin" es una técnica comparativa de valuación de negocios que involucra estimar el valor de un activo según dos escenario: uno, con cierto activo o situación en funcionamiento (la "situación," en este contexto, siendo la ocurrencia de un ataque cibernético); y el otro sin el activo o situación en funcionamiento (en este caso, la ausencia de un ataque cibernético). De la diferencia en esos estimados del valor se obtiene el valor del impacto aislado que puede ser atribuido a la situación.

Confianza en supuestos. Realizar un ejercicio de valuación o daños/pérdida a menudo requiere el uso de juicio profesional y de supuestos razonables en ausencia de datos actuales, detallados. En el análisis que el estudio realizó del impacto de un incidente cibernético en activos particulares en los escenarios hipotéticos, fueron usados referentes típicos de la industria (o investigación dirigida para identificar los referentes) a fin de llegar a supuestos para el análisis del impacto financiero. Algunos de esos supuestos aprovecharon la experiencia de Deloitte en realizar valuaciones y análisis de daños en contextos similares.

---

[1] El Ponemon Institute es reconocido como el líder en esta área por su ampliamente referenciados estudios anuales denominados *Cost of a Data Breach* [Costo de las violaciones de datos], disponibles en www.ponemon.org.

[2] "Beneath the surface of a cyberattack: A deeper look at business impacts," Deloitte Advisory, June 2016.

Contactos:

Hector Calzada
Managing Director, Deloitte Advisory Valuation Services
Deloitte Transactions and Business Analytics LLP
hcalzada@deloitte.com

John Gelinne
Managing Director, Deloitte Advisory Cyber Risk Services
Deloitte & Touche LLP
jgelinne@deloitte.com

J. Donald Fancher
National Managing Principal, Deloitte Advisory; Global Leader, Deloitte Forensic
Deloitte Transactions and Business Analytics LLP
dfancher@deloitte.com

Emily Mossburg
Principal, Deloitte Advisory Cyber Risk Services
Deloitte & Touche LLP
emossburg@deloitte.com

CFO Insights, de Deloitte, son desarrollados con la orientación del Dr. Ajit Kambil, Global Research Director, CFO Program, Deloitte LLP; y de Lori Calabro, Senior Manager, CFO Education & Events, Deloitte LLP.

Acerca del CFO Program, de Deloitte
El CFO Program reúne un equipo multidisciplinario de líderes y especialistas temáticos, de Deloitte, para ayudarles a los CXFO a mantenerse a la vanguardia de los crecientes desafíos y demandas. El programa aprovecha las capacidades amplias de nuestra organización para entregar pensamiento prospectivo e ideas frescas para cada etapa de la carrera del CFO – ayudándoles a los CFO a administrar las complejidades de sus roles, abordar los desafíos más importantes de su compañía, y adaptarse a los cambios estratégicos en el mercado.

Para más información acerca del CFO Program, de Deloitte, visite nuestro sitio web en: www.deloitte.com/us/thecfoprogram.

Síganos en **@deloittecfo**

Esta es una traducción al español de la versión oficial en inglés de**, CFO Insights – Seven hidden costs of a cyberattach – July 2016,** publicado por Deloitte Development LLC 2016 **–** Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.