MarshMcLennan

Comprender los eventos cibernéticos

Un modelo para reducir la frecuencia y aumentar la resiliencia

Marsh GuyCarpenter Mercer OliverWyman

Resumen ejecutivo

A medida que las amenazas cibernéticas se vuelven más sofisticadas y frecuentes, las empresas enfrentan el desafío de decidir cómo priorizar sus limitados recursos en ciberseguridad., incluidos los seguros, para respaldar mejor su estrategia de resiliencia.

Este informe presenta una metodología desarrollada por Marsh McLennan que permite a las organizaciones comprender, medir y gestionar mejor sus riesgos cibernéticos, a partir del uso inteligente de datos y modelos predictivos.

El estudio se basa en el desarrollo de modificadores de frecuencia, herramientas que permiten estimar la probabilidad de que una organización experimente un evento cibernético a lo largo del tiempo, en comparación con empresas de características similares en su industria.

A partir de estos indicadores de frecuencia, abordamos la pregunta fundamental:

¿Con qué frecuencia es probable que una organización sufra un evento cibernético en comparación con sus pares?

Metodología

Para estimar la probabilidad de que una organización enfrente un evento cibernético, el equipo del CRIC utilizó tres fuentes de datos:

- Análisis externos de vulnerabilidades (outside-in)
- Respuestas a los Cuestionarios de Autoevaluación Cibernética (CSA) de Marsh
- Inteligencia de amenazas, incluyendo datos de la dark web.

Estas fuentes pueden utilizarse de forma independiente o de manera combinada para construir modelos más robustos y precisos que reflejen la frecuencia de los eventos cibernéticos con mayor exactitud.

Acerca del Centro de Inteligencia de Riesgos Cibernéticos

El Centro de Inteligencia de Riesgos Cibernéticos (CRIC) de Marsh McLennan es un centro global de excelencia en datos, análisis y modelado cibernético, reconocido internacionalmente. Fundado en 2021, su misión es transformar la manera en que las organizaciones y sus comunidades anticipan, cuantifican y gestionan el riesgo cibernético desde una perspectiva económica.

*Estas fuentes pueden utilizarse de forma independiente o de manera combinada para construir modelos más robustos y precisos que reflejen la frecuencia de los eventos cibernéticos con mayor exactitud.

Hallazgos clave

Este análisis genera un "modificador de frecuencia", diseñado para estimar la probabilidad en la que una empresa puede experimentar un evento cibernético en el próximo año, en comparación con empresas similares de la industria*.

El tamaño de la organización, medido por sus ingresos, juega un papel relevante en la determinación de dicha probabilidad, lo que influye en las estrategias de gestión del riesgo:

- En las pequeñas empresas, la frecuencia de los eventos cibernéticos muestra una mayor variabilidad. Esto significa que las mejoras en sus medidas de ciberseguridad pueden tener un impacto más significativo en la reducción del riesgo.
- Por el contrario, las grandes empresas tienden a presentar menor variación en la frecuencia de eventos. Por lo tanto, los beneficios en términos de frecuencia asociados a la mejora de sus controles de ciberseguridad pueden ser más limitados. Sin embargo, debido a su mayor exposición financiera, incluso pequeñas mejoras pueden generar impactos económicos relevantes.
- Otras implicaciones relacionadas con el tamaño de la organización influye en factores como su nivel de exposición frente a ciberdelincuentes, el potencial de mejora en su postura de seguridad, las consecuencias financieras y las consideraciones asociadas al seguro..

Aunque una empresa alcance la mejor puntuación en estos indicadores, siempre existe un riesgo residual: ninguna organización está exenta de enfrentar un evento cibernético.

* Estos modificadores están integrados en el Modelo de Pérdida de Desgaste Cibernético (CALM™) 2.0 de Marsh McLennan, con el objetivo de mejorar su capacidad predictiva.

Uso de datos para priorizar las inversiones en controles cibernéticos

En 2023, el Centro de Inteligencia de Riesgos Cibernéticos (CRIC) de Marsh McLennan publicó un informe pionero en la industria, titulado "Uso de datos para priorizar las inversiones en ciberseguridad", que demuestra cómo el análisis de datos puede ayudar a las organizaciones a evaluar el impacto de sus controles de ciberseguridad. El informe también presenta aplicaciones prácticas para priorizar inversiones y desarrollar hojas de ruta estratégicas en materia de ciberseguridad.

Principales hallazgos del informe:

- Las técnicas de fortalecimiento automatizado (hardening) demostraron ser el control más efectivo, entre todos los analizados, para reducir la probabilidad de un ciberataque exitoso.
- Identificar al hardening como el control más eficaz en este ámbito resultó revelador. Hasta ese momento, los controles más valorados por el mercado asegurador eran la Detección y Respuesta en Endpoints (EDR), la Autenticación Multifactor (MFA) y la Gestión de Accesos Privilegiados (PAM).
- El informe también evidenció que la MFA tiene un impacto altamente positivo, siempre que se implemente de manera completa. Este hallazgo refuerza la importancia de adoptar un enfoque de defensa en profundidad para fortalecer la ciberseguridad.

Análisis de la frecuencia de los eventos

Hoy en día, la mayoría de las organizaciones asumen que, en algún momento, podrían enfrentar un evento cibernético. En este análisis, buscamos ir más allá de la mera posibilidad de que ocurra y enfocarnos en la frecuencia relativa, incorporando este componente clave de nuestro Modelo de Pérdida de Desgaste Cibernético (CALM™). Así, planteamos la siguiente pregunta: *¿Con qué frecuencia puede una organización experimentar un evento cibernético en comparación con empresas similares?*

Para responder esta pregunta, analizamos tres tipos de datos: análisis externos de ciberseguridad, datos del Cuestionario de Autoevaluación Cibernética (CSA) de Marsh e inteligencia de amenazas. Utilizamos esta información para calcular valores relativos que indican qué tan expuesta está una organización a experimentar un evento cibernético, en comparación con los datos de pérdidas de la industria patentados de Marsh McLennan

- Los análisis externos son una forma no intrusiva de evaluar la postura de ciberseguridad de una organización a partir de información disponible públicamente. Aplicamos modelos estadísticos para asignar a estos hallazgos una puntuación que refleja el nivel aparente de preparación de la organización frente a un ciberataque. Si bien estos análisis son útiles, de los tres tipos de datos que revisamos, son los que ofrecen menor capacidad predictiva respecto a la probabilidad de sufrir un evento cibernético
- Los datos del Cuestionario de Autoevaluación Cibernética (CSA) de Marsh se basan en miles de respuestas recopiladas, junto con datos vinculados a pólizas de seguros. Estos datos proporcionan una indicación del nivel de preparación de una organización, evaluando las medidas de ciberseguridad implementadas que podrían reducir la probabilidad de sufrir un evento cibernético.
- La inteligencia de amenazas, a menudo asociada a la dark web, refleja información que los actores maliciosos buscan, venden o compran activamente. Incluye credenciales robadas, posibles vulnerabilidades y otros datos extraídos de la dark web, sitios web y aplicaciones. Este tipo de inteligencia permite conocer qué información de una organización está expuesta en estos entornos, lo que puede ser un indicador de una mayor proximidad a sufrir un evento cibernético

Si bien cada una es una valiosa fuente de información de manera induvidual, su combinación permite construir una visión más sólida y precisa sobre la frecuencia con la que una organización podría enfrentar un evento cibernético.

El tamaño importa

En todos los sectores analizados y para las tres fuentes de datos, identificamos que el tamaño de la organización tiene una influencia significativa en los modificadores de frecuencia, lo que genera importantes implicaciones para las estrategias de gestión de riesgos cibernéticos.

En términos generales, las empresas más pequeñas tienden a mostrar una mayor variabilidad entre los escenarios de mejor y peor caso, definidos de la siguiente manera:

- **Mejor caso:** Cuando la organización declara contar con las mejores prácticas de ciberseguridad implementadas.
- **Peor caso:** Cuando la organización reporta prácticas de ciberseguridad deficientes o mínimas.

Esta diferencia es menos pronunciada en las empresas más grandes, donde los modificadores de frecuencia muestran menos variación entre ambos escenarios.

Las empresas más grandes tienden a tener una menor variación en los modificadores de frecuencia, lo que significa que parecen tener menos margen de mejora. Sin embargo, lo que está en juego desde el punto de vista financiero parece ser mucho mayor, e incluso las pequeñas diferencias pueden provocar importantes repercusiones financieras.

Principales diferencias según el tamaño de la organización:

1. Objetivo para los ciberdelincuentes

- Empresas pequeñas: Suelen ser blanco de ataques masivos o automatizados. Si un intento falla, los atacantes suelen pasar rápidamente al siguiente objetivo. Este patrón puede traducirse en una menor frecuencia de ataques dirigida específicamente a estas organizaciones, en comparación con empresas de mayor tamaño.
- Empresas grandes: Son objetivos más atractivos debido al mayor potencial económico —por ejemplo, en casos de ransomware— y por la amplitud de su superficie de ataque. Si un primer intento fracasa, los ciberdelincuentes suelen ser más persistentes, aplicando múltiples estrategias hasta lograr el acceso.

2. Potencial de mejora en ciberseguridad

- Empresas pequeñas: Generalmente cuentan con controles de ciberseguridad menos desarrollados, lo que les ofrece un mayor margen de mejora. La implementación de controles básicos puede reducir de manera significativa su probabilidad de sufrir un incidente cibernético.
- Empresas grandes: Se espera que cuenten con programas de ciberseguridad más robustos. Aunque su margen de mejora es menor, mantener elevados estándares de higiene cibernética es fundamental para gestionar los riesgos de forma efectiva.

3. Impacto financiero

- Empresas pequeñas: La diferencia entre el mejor y el peor escenario en los modificadores de frecuencia puede ser considerable. Esto significa que adoptar mejores prácticas puede reducir de forma sustancial la probabilidad de sufrir una violación de seguridad.
- Empresas grandes: Incluso pequeñas variaciones en los modificadores de frecuencia pueden traducirse en pérdidas financieras muy relevantes, debido a la magnitud de sus operaciones. Esto refuerza la necesidad de contar con estrategias integrales de gestión de riesgos.

4. Implicaciones para el seguro cibernético

- Empresas pequeñas: Deben considerar cómo las mejoras en su postura de ciberseguridad impactan su perfil de riesgo al momento de evaluar necesidades y opciones de seguro.
- Empresas grandes: Necesitan revisar detenidamente sus programas de seguros, considerando tanto la severidad como la volatilidad de los riesgos cibernéticos modelados. Esto les permitirá tomar decisiones informadas sobre los niveles de cobertura más adecuados.

Desarrollo de modificadores de frecuencia

Para cada una de las tres fuentes de datos, desarrollamos modificadores de frecuencia numéricos que permiten a las organizaciones entender cómo su perfil actual de ciberseguridad puede influir en la probabilidad de sufrir un evento cibernético. Cada modificador es una puntuación relativa que mide la frecuencia esperada de eventos cibernéticos en comparación con los pares de la organización, definidos como empresas del mismo sector y con un nivel de ingresos similar.

Combinación de modelos estadísticos

El modificador de frecuencia se construye a partir de dos modelos estadísticos que calculan la probabilidad de que ocurra un evento cibernético. Se expresa como:

$$\text{Modificador de frecuencia} = \frac{P_{\text{ingresos + industria + señales cibernéticas}}}{P_{\text{ingresos + industria}}}$$

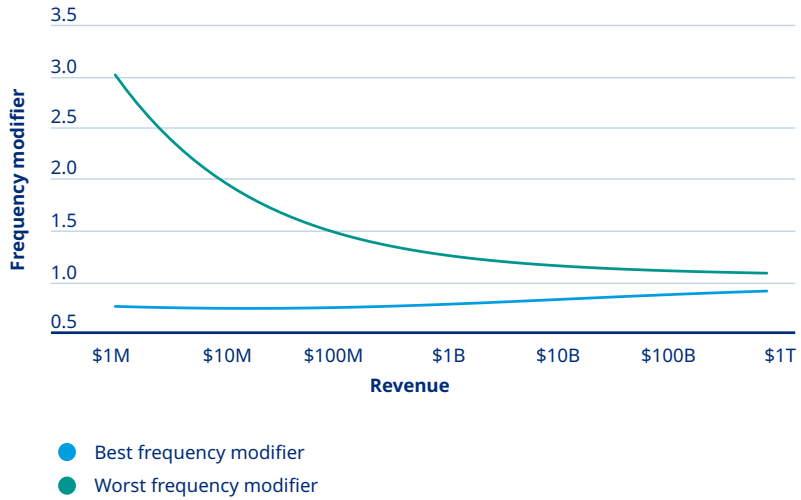
- El **numerador** representa un modelo que estima la probabilidad de un evento cibernético considerando tres factores: el nivel de ingresos, la industria y las señales cibernéticas específicas de la organización.
- El **denominador** representa un modelo base que estima la probabilidad únicamente en función de los ingresos y la industria, sin incluir las señales cibernéticas particulares.

Variantes del modificador según las fuentes de datos

Desarrollamos múltiples variantes del modificador de frecuencia en función de las señales cibernéticas disponibles, que provienen de tres tipos de datos:

- Análisis externos (outside-in) de ciberseguridad.
- Respuestas al Cuestionario de Autoevaluación Cibernética (CSA) de Marsh.
- Inteligencia de amenazas, incluyendo datos de la dark web

01| Probabilidad general de experimentar un evento cibernético



Interpretación del modificador

En todos los modelos, un valor base de **1** representa la probabilidad promedio de que una empresa genérica —con ingresos y sector similares— sufra un evento cibernético en el próximo año.

Valores superiores a 1 indican un mayor nivel de riesgo en comparación con los pares, mientras que valores inferiores a 1 sugieren un menor nivel de riesgo relativo.

(Ver Figura 1 para referencia visual)

Por ejemplo, en la industria A, eso puede significar que es probable que ocurran dos eventos cada 10 años. En la industria B, pueden ser tres eventos cada 10 años. Aplicando los datos del modelo:

- Un modificador de frecuencia por encima de 1 significa que hay una mayor probabilidad de que se produzca un evento cibernético, en comparación con sus pares.
  - En la Industria A, un modificador de 1.5 significaría que una organización probablemente experimentará 3 eventos cada 10 años (1.5 x 2, o por encima del promedio).
  - En la Industria B, un modificador de 1,5 significaría que una organización probablemente experimentará 4,5 eventos cada 10 años (1,5 x 3, o por encima del promedio).
- Un modificador de frecuencia por debajo de 1 significa que hay una menor probabilidad de un evento cibernético, en comparación con empresas similares .
  - En la Industria A, un modificador de 0.75 significaría que una organización probablemente experimentará 1.5 eventos cada 10 años (0.75 x 2, o por debajo del promedio).
  - En la Industria B, un modificador de 0.75 significaría que una organización probablemente experimentará 2.25 eventos cada 10 años (0.75 x 3, o por debajo del promedio).

A primera vista, los modificadores de frecuencia pueden parecer reflejar diferencias menores. Sin embargo, considerando que un evento cibernético puede generar pérdidas de varios millones de dólares, incluso pequeñas variaciones en la frecuencia pueden tener un impacto financiero muy significativo

La exposición en la dark web incrementa los riesgos de ciberseguridad

Una investigación reciente del Centro de Inteligencia de Riesgos Cibernéticos (CRIC) de Marsh McLennan, en colaboración con Searchlight Cyber, analizó la relación entre el riesgo de ciberseguridad de una organización y su nivel de exposición en la **dark web**, un segmento de Internet que suele ser utilizado como canal de comunicación y transacción por ciberdelincuentes.

El estudio identificó una correlación estadísticamente significativa entre la frecuencia con la que el nombre de una empresa aparece en foros de la dark web, sitios asociados a actividades maliciosas y otras plataformas utilizadas por actores de amenazas, y una mayor probabilidad de sufrir un ciberataque.

En términos simples: la presencia de cualquier hallazgo relacionado con una organización en la dark web, sin excepción, se asocia con un incremento en la probabilidad de sufrir una violación de seguridad.

El análisis también demostró que los factores externos relacionados con amenazas están directamente correlacionados con la frecuencia de los eventos de ciberseguridad, incluidas las violaciones de datos, lo que refuerza la importancia de monitorear de manera activa la exposición en estos entornos.

Análisis detallado de las tres fuentes de datos

Cada una de las tres fuentes de datos utilizadas para construir los modificadores de frecuencia tiene características particulares que aportan valor desde diferentes perspectiva.

Análisis externo de superficie cibernética

Los análisis externos son evaluaciones no intrusivas que se realizan a partir de información públicamente disponible, con el objetivo de comprender la postura de ciberseguridad de una organización.

Si bien existen decenas de métricas posibles, nuestro modelo se enfoca en tres elementos clave que evalúan aspectos críticos de la exposición cibernética de la organización:

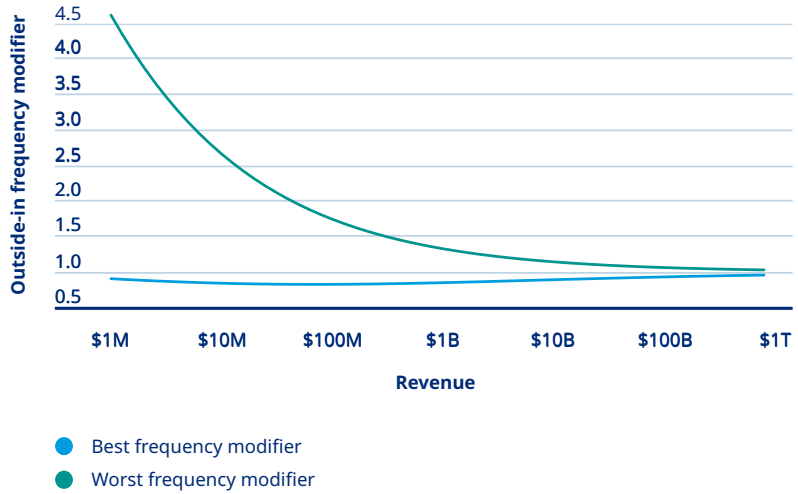
- El tiempo que tarda una organización en probar e implementar actualizaciones de seguridad.
- La presencia de software que puede no ser compatible o que puede estar desactualizado.
- La posibilidad de que un dispositivo de la red de la organización esté ejecutando un programa o una aplicación que puede que no se desee o que no debería estar ejecutándose.

El modificador de frecuencia basado en análisis externos considera tres factores: los ingresos de la organización, su industria y los resultados de los análisis externos o análisis outside-in. (Ver Figura 2):

$$\textit{Modificador de frecuencia outside - in} = \frac{P_{ingresos+industria+outsine\ in}}{P_{ingresos+industria}}$$

Como se mencionó anteriormente, los datos provenientes de análisis externos (outside-in) son los menos predictivos en términos de estimar la probabilidad de que ocurra un evento cibernético. Sin embargo, siguen siendo útiles para identificar áreas con potencial de mejora en la postura de ciberseguridad. A partir de los hallazgos específicos de cada organización, asignamos una puntuación que se integra al modelo como parte del modificador de frecuencia basado en análisis externos.

02| **Datos externos (outside-in)**



El gráfico anterior muestra cómo varía el modificador de frecuencia basado en análisis externos para empresas de diferentes tamaños en esta industria:

Para una empresa con ingresos de **1.000 millones de dólares**

- Tener la **peor puntuación** en análisis outside-in genera un modificador de frecuencia de aproximadamente **1.3** (por encima del promedio),
- Mientras que la **mejor puntuación** en análisis outside-in reduce el modificador a aproximadamente **0.83** (por debajo del promedio).

Para una empresa de **100.000 millones de dólares:**

- Tener la peor puntuación de análisis outside-in, genera un modificador de frecuencia de aproximadamente 1.05 (por encima del promedio).
- Tener la mejor puntuación de análisis externo, outside- in generará como resultado un modificador de frecuencia de aproximadamente 0.97 (por debajo del promedio).

Datos de autoevaluación cibernética

El CSA de Marsh es un conjunto completo de preguntas sobre las medidas de ciberseguridad que los clientes completan (voluntariamente). Las preguntas cubren temas que se alinean con los 12 controles clave de Marsh (agregue un enlace UTM) y que tocan áreas que incluyen:

- Gestión del control de acceso
- Protección de datos
- Gestión de la infraestructura de red

Desarrollamos modificadores de frecuencia para organizaciones que reportan las mejores prácticas de ciberseguridad en sus respuestas al Cuestionario de Autoevaluación Cibernética (CSA), así como para aquellas que reflejan prácticas deficientes en sus respuestas (véase la Figura 3). El modificador de frecuencia basado en inteligencia de amenazas considera tres factores: los ingresos de la organización, su industria y los resultados del Cuestionario de Autoevaluación Cibernética (CSA):

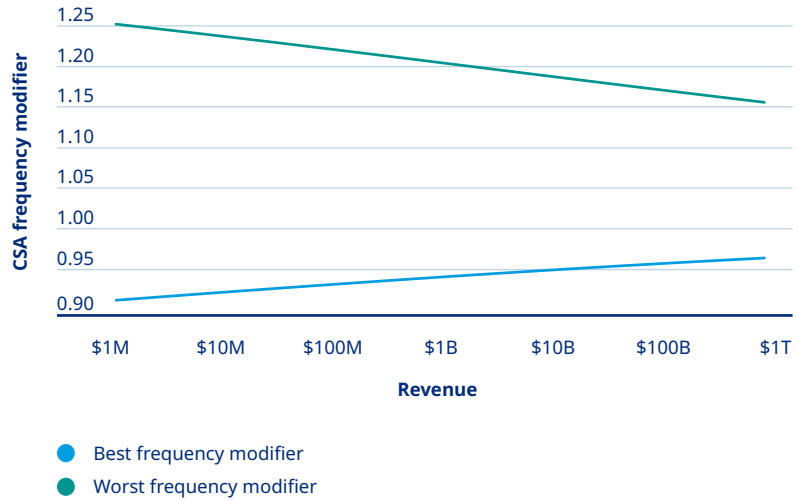
$$\textit{Modificador de frecuencia CSA de Marsh} = \frac{P_{revenue + industry + CSA}}{P_{revenue + industry}}$$

En el caso (improbable) de que una empresa tuviera todas las respuestas "incorrectas" al CSA, el modificador de frecuencia de eventos para una empresa con ingresos de 1 millón de dólares sería 1.6. El mejor de los casos sería 0.75.

Al igual que con los datos de afuera hacia adentro, la brecha entre los modificadores para el peor y el mejor caso es menor para las empresas de mayores ingresos: en este ejemplo, para una empresa de 100 mil millones de dólares serían 1.25 y 0.82, respectivamente. El tamaño de la brecha para los datos de CSA es mayor que el de los datos de afuera hacia adentro, lo que indica que los datos de CSA pueden estar más correlacionados con la frecuencia de incidentes cibernéticos que los datos de afuera hacia adentro.

Una brecha más grande para el "gráfico de embudo" de CSA implicaría que el efecto en su ciberseguridad de mejorar sus respuestas de CSA es mayor que el efecto de mejorar sus puntajes de escaneo de afuera hacia adentro (outside-in).

03| Datos de la CSA de Marsh



Datos de inteligencia de amenazas

La tercera área que modelamos para este estudio, la inteligencia de amenazas busca menciones en la dark web o en otros sitios web y aplicaciones que se sabe que tienen una conexión con la actividad de los actores de amenazas, incluidas las credenciales robadas que están a la venta. Se ha demostrado que dicha exposición es predictiva de una mayor posibilidad de que una organización sea objeto de un evento cibernético.

El modificador de frecuencia de inteligencia de amenazas tiene en cuenta los ingresos, el sector y la inteligencia de amenazas (consulte la figura 4):

$$\textit{threat intelligence frequency modifier} = \frac{P_{\textit{ingresos + industria + inteligencia de amenazas}}}{P_{\textit{ingresos + industria}}}$$

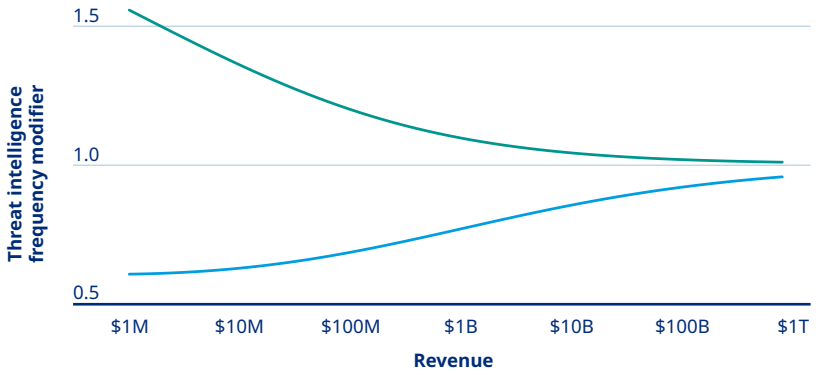
Al igual que con nuestros modelos outside-in y CSA, los modificadores de frecuencia para el peor y el mejor de los casos adquieren forma de embudo a medida que aumenta el tamaño de la empresa.

Combinación de fuentes de datos

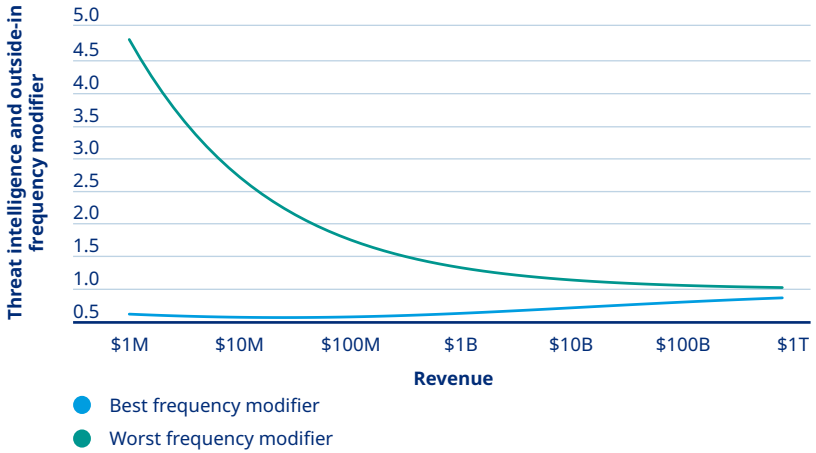
A menudo, combinamos los datos de inteligencia sobre amenazas con los análisis outside-in (consulte la figura 5) y nos referimos a los dos juntos como datos tecnológicos.

$$\textit{Modificador de frecuencia tecnográfico} = \frac{P_{\textit{ingresos + industria + datos demográficos}}}{P_{\textit{ingresos + industria}}}$$

04| Inteligencia de amenazas



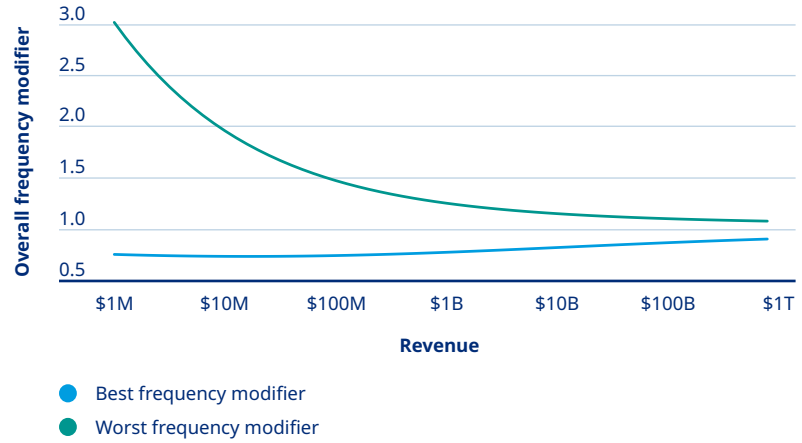
05| Modelo combinado de inteligencia de amenazas y análisis externo (outside-in)



Cada uno de los tres modelos —outside-in, CSA e inteligencia de amenazas— aporta información única. Al combinarlos, obtenemos un modificador de frecuencia consolidado que ofrece una evaluación integral del riesgo cibernético. (consulte la Figura 6).

$$\textit{Modificador de frecuencia general} = \frac{P_{\textit{ingresos + industria+datos tecnográficos + CSA}}}{P_{\textit{ingresos + industria}}}$$

06| Modificador de frecuencia general



Conclusión

La compra de un seguro cibernético como parte de su estrategia de resiliencia está respaldada por nuestro análisis de datos de frecuencia, que muestra que el riesgo de un evento cibernético no se puede reducir a cero. Además, el análisis de gravedad puede respaldar su decisión sobre la cantidad de seguro que debe comprar.

Es fundamental que las organizaciones revisen la eficiencia de su programa de seguros en el contexto de las pérdidas potenciales modeladas, ya que esto permite una mejor comprensión de la gravedad y la volatilidad de los riesgos cibernéticos específicos.

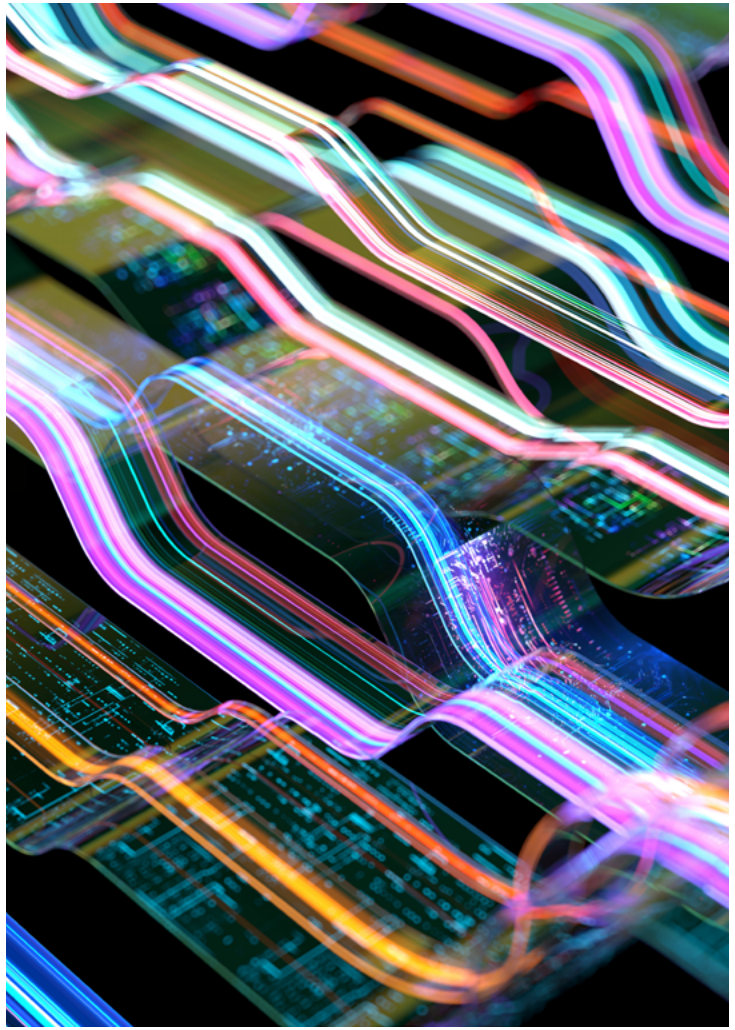
Al analizar conjuntamente los datos provenientes de análisis externos (outside-in), las respuestas al Cuestionario de Autoevaluación Cibernética (CSA) de Marsh y los hallazgos de inteligencia de amenazas — en comparación con nuestra base de datos de pérdidas patentada— podemos estimar la probabilidad de que una organización experimente una pérdida asegurada por riesgo cibernético a lo largo del tiempo, en relación con empresas de características similares.

Si bien cada una de estas tres fuentes aporta valor por sí sola, su combinación permite construir un modelo más robusto y preciso para evaluar el riesgo cibernético.

Los resultados de este estudio se utilizan en nuestro Modelo de Pérdida de Desgaste Cibernético para ayudarlo a modelar con mayor precisión la frecuencia probable con la que su organización experimentará una pérdida cibernética y para encontrar áreas para implementar varios controles en un intento de disminuir esa frecuencia. Estos modelos no solo son útiles para la planificación de la resiliencia, sino que también utilizan datos que generalmente están disponibles para las aseguradoras y que los suscriptores pueden utilizar para informar las decisiones relacionadas con la cobertura y los precios.

En Marsh McLennan, su organización puede evaluar tanto el riesgo financiero asociado a su postura actual de ciberseguridad como los beneficios económicos de fortalecerla. Además, este enfoque permite optimizar la decisión sobre los niveles de cobertura de seguro cibernético, ajustándola a su apetito de riesgo.

Para obtener más información, comuníquese con su representante de Marsh, Guy Carpenter u otro representante de Marsh McLennan.



MarshMcLennan

Marsh GuyCarpenter Mercer OliverWyman