MARSH RISK CONSULTING

SEGURIDAD CIBERNÉTICA
CONSULTORÍA Y ASESORAMIENTO

SERVICIOS DE GESTIÓN DE RIESGOS DE SEGURIDAD CIBERNÉTICA

RISK. DISPUTES. STRATEGY.

MARSH

Los negocios en el siglo XXI están tan conectados a la tecnología que una nueva verdad ha emergido: Las organizaciones están casi constantemente bajo un ataque cibernético. Los recursos digitales que transforman la industria crean riesgos distintos a cualquiera con los que han confrontado antes. Los actores de la amenaza sofisticada, incluyendo estados nacionales, crimen organizado, y grupos organizados de hackers y personas particulares, atacan su sistema directamente o a través de terceras personas con herramientas y métodos siempre en permanente evolución.

Las intrusiones e infracciones de datos cibernéticos sitúan a la información crítica empresarial, a la propiedad intelectual, a los datos financieros, y a la información de identificación personal en riesgo, lo que puede conducir a interrupciones del negocio, robo y fraude, daño a la reputación, y otros impactos adversos. Prepararse para responder efectivamente este riesgo requiere un esfuerzo coordinado en toda su organización.

La Gestión de Riesgos de Seguridad Cibernética de Marsh Risk Consulting (MRC) Services hace frente a los elementos principales de la seguridad cibernética, desde estrategia, gobernanza, la gestión de riesgos institucionales, para controlar la arquitectura, implementación y gestión. Nuestros servicios y nuestros conocimientos prácticos hechos a la medida para su entorno y necesidades específicas de su empresa, lo ayudan a tomar decisiones informadas de gestión de riesgos en cuanto a la seguridad cibernética y mejoran su capacidad de recuperación de las siempre presentes amenazas cibernéticas.

LAS CIFRAS DE CIBER

$445 millones:
Costo estimado del crimen cibernético a la economía global.

$120 millones:
Tamaño esperado del mercado cibernético global en el 2017.

40 milliones:
La cantidad de personas en los EE.UU. a quien los hackers les han robado información en el 2014.

$5.85 million:
Costo promedio de infracciones en los EE.UU.

10%:
Incremento sobre el año pasado en el costo promedio de mitigación de infracción (incluyendo costos de detección e incremento post-infracción y lucro cesante

$417,000:
Costo promedio de detección y de incremento.

LO DESTACADO DEL SERVICIO

La gestión efectiva de riesgo de seguridad cibernética empieza desde arriba, derivando del liderazgo y experticia de directivos en todos los departamentos de la organización. Requiere que la atención de los líderes sea dirigida a:

- Establecer un programa cultural, ambiental, y orgánico de gestión de riesgos cibernéticos impulsado por datos veraces basados en un conocimiento refinado de la tolerancia a los riesgos y apetito de la organización.
- Asegurar que los objetivos y políticas del programa reflejen y apoyen los requerimientos de la empresa.
- Crear un ambiente de controles de seguridad cibernética de controles administrativos, físicos, y técnicos que implementen la política.
- Desarrollar una fuerza laboral que tenga la capacidad y habilidades necesarias para impulsar la configuración, operación, y monitoreo continuo de los controles de seguridad, como también las habilidades y recursos para responder a las alertas de seguridad.
- Logrando un estándar alto para la capacidad de identificación de los incidentes cibernéticos y capacidad de respuesta, incluyendo la detección, análisis inicial, incremento, contención, erradicación y recuperación.

Conociendo su actitud de seguridad cibernética dentro del contexto de sus amenazas cibernéticas, incluyendo las amenazas inherentes de riesgos cibernéticos de terceros, es el primer paso crítico y está en el núcleo de nuestras ofertas de servicio.

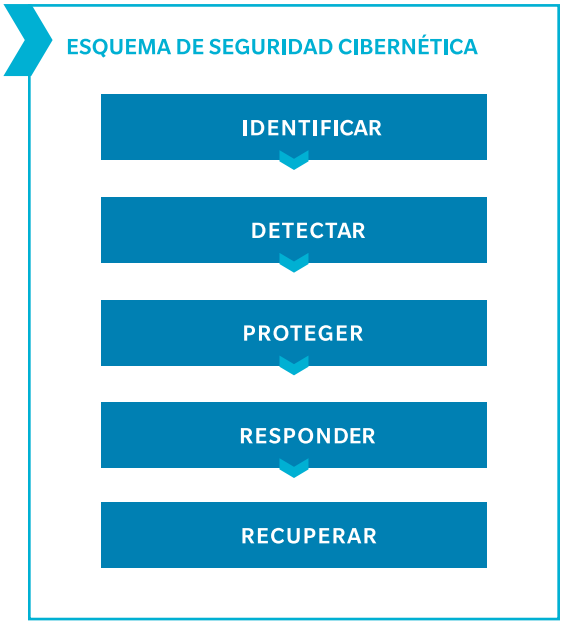
Los servicios integrados esbozados a continuación son la fundación de lo mejor de su clase del programa de la gestión de riesgos de seguridad cibernética. Hacemos estas ofertas a la medida de sus necesidades y las alineamos al entorno del negocio de su organización para que usted comprenda mejor y afronte las amenazas cibernéticas de hoy y mañana.

Evaluación de Programa de Seguridad Cibernética a Nivel Institucional

El punto de partida para la gestión de riesgos de seguridad cibernética consiste en la evaluación de su programa actual utilizando estándares y esquemas nacionales reconocidos a nivel global. Los expertos de MRC revisarán todo su programa de seguridad cibernética a nivel institucional contra esquemas respetados a nivel de programa tales como:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- ISO 27000 - Series Estándar.
- HIPAA Regla de Seguridad.
- Center for Internet Security Critical Security Controls.

Nuestra propia metodología de evaluación está basada en una síntesis para clientes específicos de estos y otros estándares de referencia con nuestras propias y únicas herramientas de análisis.



Nuestra propia metodología de evaluación sintetiza los principales esquemas de seguridad cibernética, las herramientas exclusivas de Marsh, consultoría y análisis de campo la base para una gestión de riesgos estratégicos y para una hoja de ruta para la inversión.

Nuestra captura de datos sigue un proceso estructurado de entrevistas personales con ejecutivos senior, desde el CEO hasta el CISO, Gerentes, y personal de operaciones. Además revisamos su actual programa de documentación, estudiamos sus instalaciones, y de manera objetiva establecemos parámetros de su posición de seguridad contra sus pares en la industria usando nuestras herramientas especializadas de análisis de datos en gran escala. En nuestro análisis, evaluamos el grado en que los resultados definidos de seguridad del Esquema de Seguridad Cibernética NIST, por sus siglas en inglés) (u otros esquemas, según proceda) se están confrontando mediante la aplicación de medidas objetivas, incluyendo criterios de pruebas de control de NIST SP 800-53 y nuestras propias herramientas.

Los resultados y recomendaciones que emanen de este análisis representan el primero de dos proyectos mayores de entregables. Informan sobre la hoja de ruta estratégica multianual que constituye el segundo entregable significativo. Esta hoja de ruta, desarrollados a través de uno o más talleres colaborativos con CISO y CIO, gestión de riesgo, y otras partes interesadas, está diseñada para constituir el formulador de la agenda estratégica y un cronograma para su el programa de seguridad cibernética de su organización para unos tres o cinco años.

Revisión de Seguridad de Controles Técnicos

A medida que usted despliegue y gestione controles de seguridad y aplicaciones para combatir el riesgo cibernético, es fácil perder de vista la efectividad de las inversiones realizadas. ¿Cómo encajan los controles existentes con las verdaderas prioridades de la organización? ¿Cuál es el impacto de adquisiciones, consolidaciones, o reestructuración en el entorno de sus controles?

Nuestra revisión metódica del entorno de sus controles técnicos de seguridad cibernética le ayuda a conocer mejor:

- Qué tan bien sus controles aplican su política.
- Qué tan eficientemente sus controles manejan su apetito de riesgos.
- Qué tan efectivamente sus controles cumplen con los requisitos.

Nuestra metodología repetitiva y rastreadora se basa en estándares aceptados de controles técnicos de seguridad tales como los del Center for Internet Security Critical Security Controls, NIST SP 800-53, HIPAA, PCI DSS y otros estándares para sectores específicos.

Al igual que el programa de evaluación pero específicamente enfocado en la evaluación de la eficacia de los controles técnicos, nuestra captura de datos sigue un proceso estructurado que incluye entrevistas personales con ejecutivos senior, gerentes, y personal de operaciones; inspecciones en el sitio de sus instalaciones, revisiones técnicas y de su programas, bitácoras de su sistema, controles de acceso, y documentación sobre configuraciones de dispositivos; y un análisis de alternativas de inversión por medio de técnicas analíticas avanzadas.

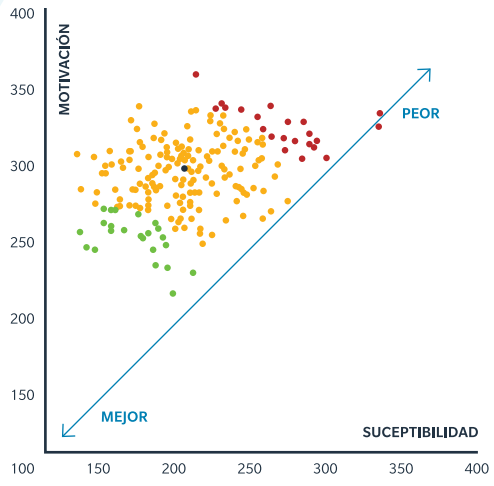
Al final de la revisión, entregamos un informe integral, incluyendo un plan de acción para las correcciones para establecer las prioridades identificadas.

Revisión de Gestión de Riesgos de Seguridad Cibernética de Terceros

La Gestión de Riesgos de Seguridad Cibernética no debe ser prioridad únicamente para su organización sino para vendedores y otros terceros con quienes usted participa también. Los incidentes recientes de seguridad cibernética demuestran a terceros la vulnerabilidad de las compañías. En algunos casos los vendedores eran los custodios de los datos hackeados e infraestructura, en otros casos le facilitaban una puerta de entrada para un ataque a una red corporativa.

Nuestra evaluación a la seguridad cibernética de terceros le puede proporcionarle a usted un esquema y las herramientas para conocer mejor y gestionar los riesgos clave asociados a terceros que tienen acceso a su red de datos, o infraestructura. Nuestros expertos lo ayudan a identificar las relaciones con terceros incluyendo las relaciones con con los suplidores y proveedores de servicio, socios del negocio, contratistas, y vendedores y a evaluar las probabilidades de infracciones o interrupciones del negocio y la severidad potencial del impacto. Nosotros destacamos tales áreas como riesgos de concentración de suplidores, lo que ocurre cuando múltiples suplidores comparten los proveedores de hosting, vendedores de seguridad, vulnerabilidades o sistemas de tecnología. Tales situaciones pueden conducir a un escenario en donde muchos proveedores fallan a la vez, exponiendo a su empresa a interrupciones e infracciones. Además podemos ayudar a desarrollar una metodología para evaluar la seguridad de nuevos proveedores que se integran.

VENDEDORES, PROVEEDORES DE SERVICIOS TERCERIZADOS, SOCIOS EMPRESARIALES



Nuestra revisión se compromete con:

- Captura de datos a través de entrevistas personales con sus equipos de compras, seguridad de la información, y gestión de riesgos para conocer los procesos existentes de gestión y las necesidades de datos.
- Un estudio dentro de su organización, de ser necesario, que identifique las relaciones con todos los proveedores y con terceros, cómo y cuándo sus riesgos han sido evaluados, y otra información empresarial pertinente.
- Desarrollo de esquema de gestión de riesgos que incluya su exposición a cada proveedor y el riesgo de infracción o interrupción del negocio y acciones recomendadas.
- Identificación de proveedores de alto riesgo, cuya vulnerabilidad de seguridad cibernética pudría ser evaluada más a fondo.

La información recabada lo ayudará a conocer mejor cuán seguros están sus datos, sus redes y su infraestructura con relación a sus vendedores y otras terceras personas, como también cuán motivados pueden estar los atacantes para hacer su explotación. Los resultados le ayudarán a gestionar mejor el riesgo de seguridad de vendedores y otras terceras personas e instituir cambios de política y acciones correctivas por parte de vendedores incumplidos.

Sobre una base de subscripción en curso, por medio de nuestra plataforma de datos masivos, podemos proporcionarle datos de evaluación de riesgo y alertas sobre la actitud de sus vendedores en cuanto a la seguridad cibernética. Esto le ayudará a manejar estas exposiciones y le permitirá a usted hacer los ajustes como sea necesario, de manera que las cuestiones emergentes de ellos no se conviertan en sus problemas de seguridad y de empresa. Adicionalmente, nuestros expertos pueden asistirlo con la evaluación e investigación a nuevos vendedores.

Ejercicios Cibernéticos Basados en Hipótesis

Considerando la frecuencia y potencial severidad de los eventos cibernéticos su organización debiera tener un plan de respuesta eficaz establecido, incluyendo el señalamiento de qué responsabilidades recaen sobre cada persona o departamento. Hacer esto puede minimizar el los tiempos de inactividad, reducir costos, reducir impactos adversos a la marca y a la reputación, y puede mejorar su perfil integral de riesgos cibernéticos.

Nuestros ejercicios de simulación puestos a la disposición al nivel ejecutivo se enfocan en su respuesta a un hipotético incidente cibernético, ayudando así a mejorar su preparación y capacidad para responder. Nuestra capacitación basada en simulación:

- Implica a aquellos responsables por la gestión de crisis e incidentes cibernéticos.
- Ofrece simulaciones cibernéticas realistas que son hechas a la medida de su entorno, sus necesidades, y los objetivos acordados del ejercicio.
- Supuestos de la pruebas, planes, y procesos operativos.
- Resalta la comprensión y concienciación de las complejidades del manejo de los incidentes cibernéticos.
- Mejora las habilidades y capacidades de sus ejecutivos y gerentes.

Para estos ejercicios, nuestros expertos en cibernética, gestión de crisis, y diseño de juegos trabajan conjuntamente con su equipo para desarrollar una serie completa de materiales de capacitación. Esto incluye una reunión informativa interna; movidas, e impulsos; guion de los jugadores; papeles [roles] y asignación de responsabilidades; una reunión informativa externa que recoja los éxitos y oportunidades para mejorar.

Tras el ejercicio nuestro equipo recomendará mejoras a su estrategia y planes de gestión de riesgos de seguridad cibernética. Para ayudarlo a que su estrategia y planes permanezcan viables, podemos establecer un programa de ejercicio en curso diseñado en torno a sus objetivos estratégicos y a incorporar simulaciones que den cuenta de los más recientes incidentes cibernéticos.

INTERRUPCIÓN OPERACIONAL
¿Qué está haciendo para mitigar riesgos en cada punto de contacto en todos sus terceros proveedores/suplidores?

CUMPLIMIENTO DE NORMAS
¿Qué cambios ha hecho recientemente en cuanto a cómo maneja y protege datos sensitivos?

EXPOSICIÓN DE LOS EMPLEADOS
¿Qué está haciendo para proteger la información del empleado clave o empleado potencial. ¿Cómo ha impactado esto su capacidad de reclutar o retener el talento?

DEMANDAS Y PERJUICIO A LA REPUTACIÓN
¿Tiene usted un plan de respuesta en el caso de infracción? ¿Cómo está usted mitigando el daño potencial?

Para conocer más acerca de estos servicios y nuestra gama completa de capacidades en consultoría y asesoramiento en seguridad cibernética y cómo lo puede ayudar a proteger sus valiosos recursos de información y a manejar los riesgos cibernéticos a nivel empresarial, favor ponerse en contacto con su representante local de Marsh o con:

THOMAS FUHRMAN
MANAGING DIRECTOR
+1 703 731 8540
thomas.fuhrman@marsh.com

JAMES HOLTZCLAW
SENIOR VICE PRESIDENT
+1 703 547 7784
james.holtzclaw@marsh.com

BRANNAN JOHNSTON
MANAGING DIRECTOR
+1 212 345 9698
brannan.johnston@marsh.com

RUSS HAWKINS
MANAGING DIRECTOR
+1 212 345 5869
russell.d.hawkins@marsh.com

RAMÓN ALONZO
MRC LEADER PANAMÁ
+507 6112 8935
ramon.alonzo@marsh.com

Para información adicional:
www.marshriskconsulting.com
www.marsh.com