Aon's Cyber Insurance Snapshot

Ayudando a las organizaciones a entender mejor los retos de los riesgos y los seguros en 2021.

AON
Empower Results®

Aon's Cyber Insurance Snapshot

Ayudando a las empresas a entender mejor los retos de los riesgos y los seguros en 2021.

En 2021, esperamos un año de dinámica de mercado cibernético fluido. Mientras ayudamos a los clientes a navegar por un duro ciclo de mercado, reconocemos la necesidad de ser proactivos en las colocaciones con un proceso de suscripción más diligente, así como la necesidad de considerar opciones de cobertura y estructuras de programas creativos para ayudar a cumplir los objetivos de transferencia de los riesgos.

Nuestro objetivo, al ofrecer una instantánea del mercado de ciberseguros de 2021, es apoyar a las organizaciones de EMEA aportando un contexto a los desafíos –tanto cuantitativos como cualitativos– que las aseguradoras están tratando de gestionar, compartir datos sobre las tendencias del mercado junto con las orientaciones de futuro ofrecidas por las aseguradoras de ciberseguros, y preparar a las organizaciones de EMEA mientras se acercan al mercado en lo que probablemente será el año más desafiante hasta la fecha en la historia de los seguros de ciber riesgos.

A lo largo de 2020, las aseguradoras alcanzaron, y en muchos casos superaron, un punto de inflexión a medida que la frecuencia y la gravedad de los siniestros superaban la mejora de la selección de riesgos y el aumento limitado de las primas. El cambio que se ha estado desarrollando desde finales de 2018, y que finalmente inclinó la balanza en 2020, se relaciona con la actividad del *ransomware* en todos los segmentos de empresas, pero principalmente en el espacio del mercado medio.

Las tendencias clave de 2020:

Frecuencia de siniestralidad - Aon's Cyber Solutions registró durante 2020 una cadencia de 3 nuevos siniestros por día hábil, a nivel mundial. Esto es un incremento de casi el 100% con respecto 2019, y casi todos ellos relacionados con *ransomware*.

Siniestralidad de impacto – El impacto medio de las pérdidas aumentó cada trimestre de 2020. En muchos casos, las pérdidas relacionadas con *ransomware* llegaron a ser de ocho cifras. Muchos de estos siniestros todavía siguen ajustándose a lo largo del año, a medida que se revisan las posteriores pérdidas por interrupción de la actividad y se litigan las reclamaciones por responsabilidad.

Primas – Aunque el incremento medio de prima entre 2019 y 2020 fue del 5% – 10%, éstos no han sido suficientes para compensar el aumento de la frecuencia y el impacto de los siniestros.

Selección del riesgo – Los Aseguradores han estado reforzando, durante 2020, las herramientas a su alcance que les ayude en la selección del riesgo. Muchos están utilizando los *cyber scan* para buscar vulnerabilidades que puedan ser objeto de ciberamenazas, y muchos han incluido nuevos cuestionarios específicos sobre *ransomware.* Estos esfuerzos se centran en mejorar los controles de los riesgos asegurados, así como en mejorar la selección de riesgos.

Prevemos que estas tendencias se van a mantener a lo largo de 2021 a un ritmo acelerado. Aon's Cyber Solutions ha recibido, por parte de los principales Aseguradores, orientación de incrementos de prima de entre el 20% y el 50%. Para mantener un compromiso estable a largo plazo con la capacidad destinada al riesgo cyber, los Aseguradores están revisando las áreas de las carteras en las que se necesita una acción de suscripción, y reevaluando el despliegue de la capacidad, específicamente en lo relacionado con las pérdidas por *ransomware.*

Tendencias de riesgo a tener en cuenta.

Trabajo en remoto

El teletrabajo ha llegado para quedarse, aumentando las vulnerabilidades potenciales dado el software del Remote Desktop Protocol (RDP), la seguridad del acceso remoto, la dependencia de terceros proveedores de servicios de IT y la comunicación digital como el principal medio para compartir información.

Ciber Extorsión

El robo y el uso indebido de información personal identificable ya no es la gallina de los huevos de oro de los cibercriminales. Los ataques de *ransomware* han evolucionado para incluir no sólo el cifrado de datos sensibles (incluida la IPP y la información corporativa confidencial) sino también la amenaza de exposición de dichos datos en Internet. Este tipo de ataques puede dar lugar a tiempos de inactividad de la empresa debido a las redes cifradas, así como a posibles consecuencias de responsabilidad en términos de sanciones administrativas o demandas de terceros.

Incumplimiento de la normativa

El entorno normativo sigue creciendo en complejidad. Las recientes multas impuestas en virtud del Reglamento General de Protección de Datos (RGPD) de la Unión Europea demuestran que las organizaciones deben ser conscientes del impacto de una violación de datos.

Más de 160.000 violaciones de datos se han notificado en los 28 países de la Unión Europea más Noruega, Islandia y Liechtenstein desde que el GDPR entró en vigor el 25 de mayo de 2018. Las sanciones aumentaron casi un 40% en 2020, alcanzando la cifra de 158,5 millones de euros, siendo la mayor sanción de 35 millones de euros emitida por el regulador alemán. El regulador italiano impuso más de 60 millones de euros en multas agregadas por el RGPD. La sanción más elevada hasta la fecha sigue siendo la de 50 millones de euros impuesta por el regulador francés.

La evolución en este ámbito podría traer consigo mayores problemas financieros desde el punto de vista de las multas y sanciones. La Ley de Protección de la Información Personal (POPIA) entró en vigor en Sudáfrica el 1 de julio de 2020, para regular el tratamiento de la información personal en consenso con las normas internacionales de privacidad.

Riesgo del proveedor

A medida que las organizaciones continúan adaptándose al entorno empresarial actual y a las necesidades del mercado asociadas, la dependencia de la tecnología de terceros y de las aplicaciones de *back-end* son mayores que nunca. Las normas de ciberseguridad de los proveedores son una parte fundamental de esta ecuación.

El compromiso de SolarWinds y las recientes vulnerabilidades de Microsoft Exchange demuestran la complejidad de las relaciones con los proveedores de tecnología y cómo aumenta el riesgo frente a la ciberseguridad.

Tecnología no cubierta

COVID-19 ha acelerado las iniciativas de transformación digital de muchas organizaciones. La aparición de servicios y productos tecnológicos en sectores más tradicionales representa una exposición de IP potencialmente "descubierta" que puede no estar contemplada desde el punto de vista de la responsabilidad y las pérdidas financieras.

1 Source: Insights publication research from DLA Piper; https://www.enforcementtracker.com/

Tendencias en la prima

Cambios en la tasa de resultados en la cartera Q4 2020 vs Q1 2021

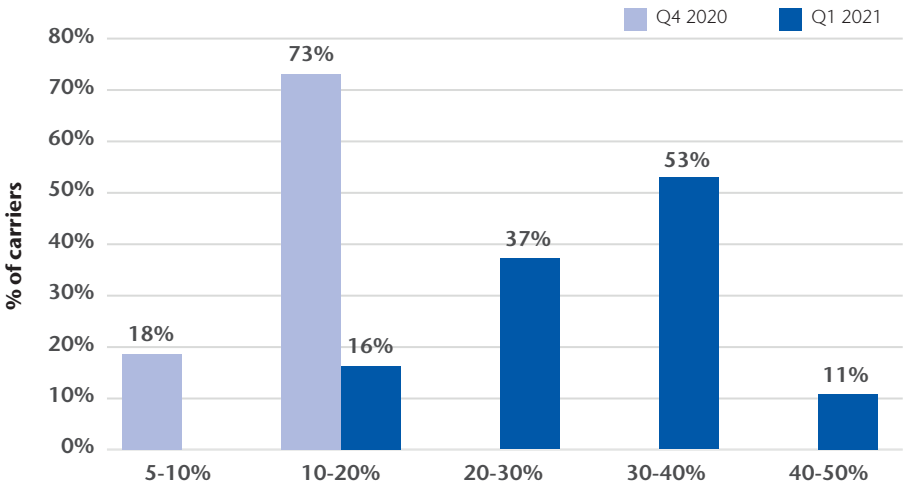
Comentarios:

Los datos de prima son en tiempo real sobre una base histórica y examinan el cambio de precios interanual sobre una base trimestral.

n Q4 2020 la tasa media de los aseguradores fue del 12%

n Q1 2021 la tasa media de los aseguradores fue del 35%, lo que representa un aumento del 23% con respecto al trimestre anterior.

Las tasas en Cyber están cambiando rápidamente.



*La orientación se proporciona a través de un estudio propio de Aon sobre los principales Aseguradores en Cyber con los que negocia Aon. No se trata de una propuesta de primas ni de una orientación específica para la propuesta de un programa de un asegurado concreto. Se trata de una orientación a nivel de cartera ofrecida por los suscriptores que participaron en la encuesta.

Fuente: Aon EMEA Cyber Carrier Survey Q1 2021

Orientación prospectiva

Orientación de las tasas en la cartera (Q1 2021)

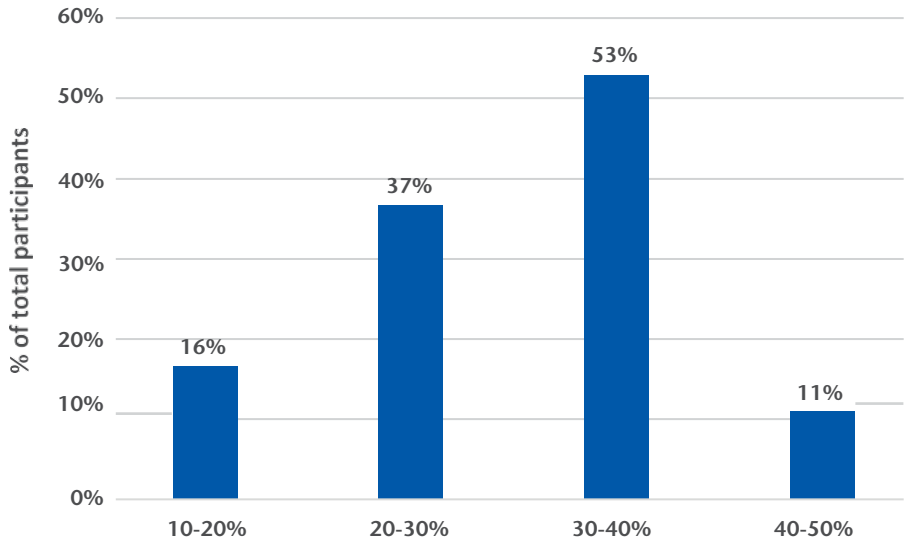
Comentarios:

Aon publica una encuesta trimestral sobre los principales suscriptores en Cyber. A continuación se presentan algunas dinámicas de primas clave que se perciben para 2021:

- La mayoría de los encuestados sugieren que las tarifas sufrirán **aumentos superiores al 30% durante Q2 2021.**

Esta información se basa en:

- Los objetivos de tasas globales de una aseguradora para su cartera. Cada asegurado tiene un perfil de riesgo ligeramente distinto. Es importante trasladar al asegurador como un asegurado en concreto está mejora preparado para gestionar sus riesgos cibernéticos.
- Ninguno de los aseguradores que contestaron sugirió que la tasa sería inferior al 10% anual en el Q2 2021.
- Aon anticipa que los precios serán variables durante 2021.



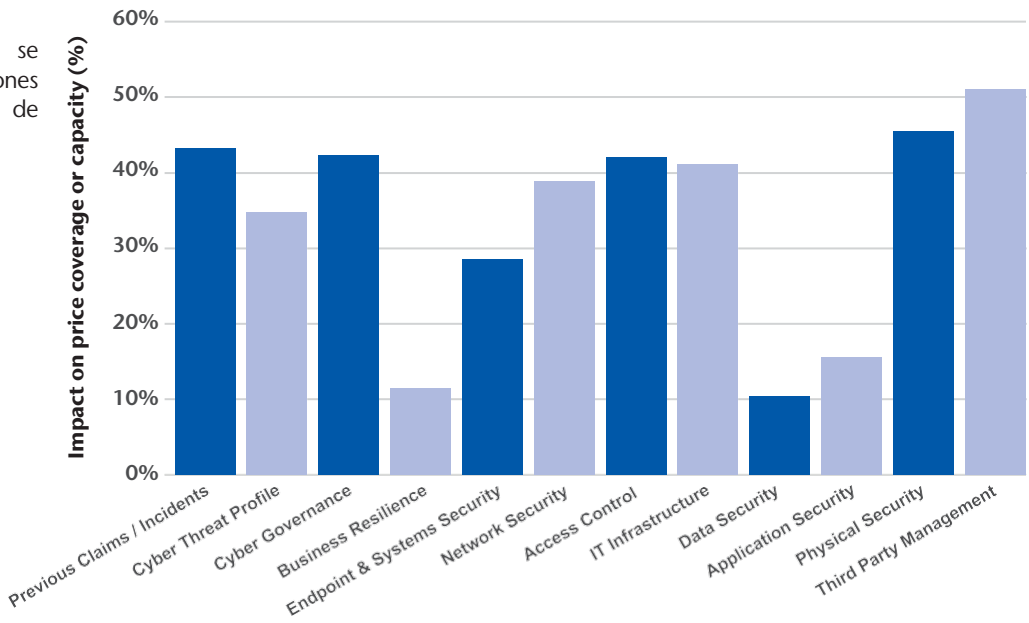
*La orientación se proporciona a través de un estudio propio de Aon sobre los principales aseguradores en Cyber con los que negocia Aon. No se trata de una propuesta de primas ni de orientaciones específicas para el programa de un asegurado concreto. Se trata de una orientación a nivel de cartera ofrecida por los suscriptores que participaron en la encuesta.

Fuente: Aon EMEA Cyber Carrier Survey Q1 2021

Puntos clave en la suscripción

Comentarios:

- Estos puntos clave se basan en las orientaciones de los aseguradores de cara al futuro.
- Estos puntos muestran la importancia del proceso de suscripción, aunque no se limitan solo a estos aspectos, sino que deben considerarse como punto de partida para las discusiones de suscripción basadas en la exposición a riesgos específicos del sector e individuales.

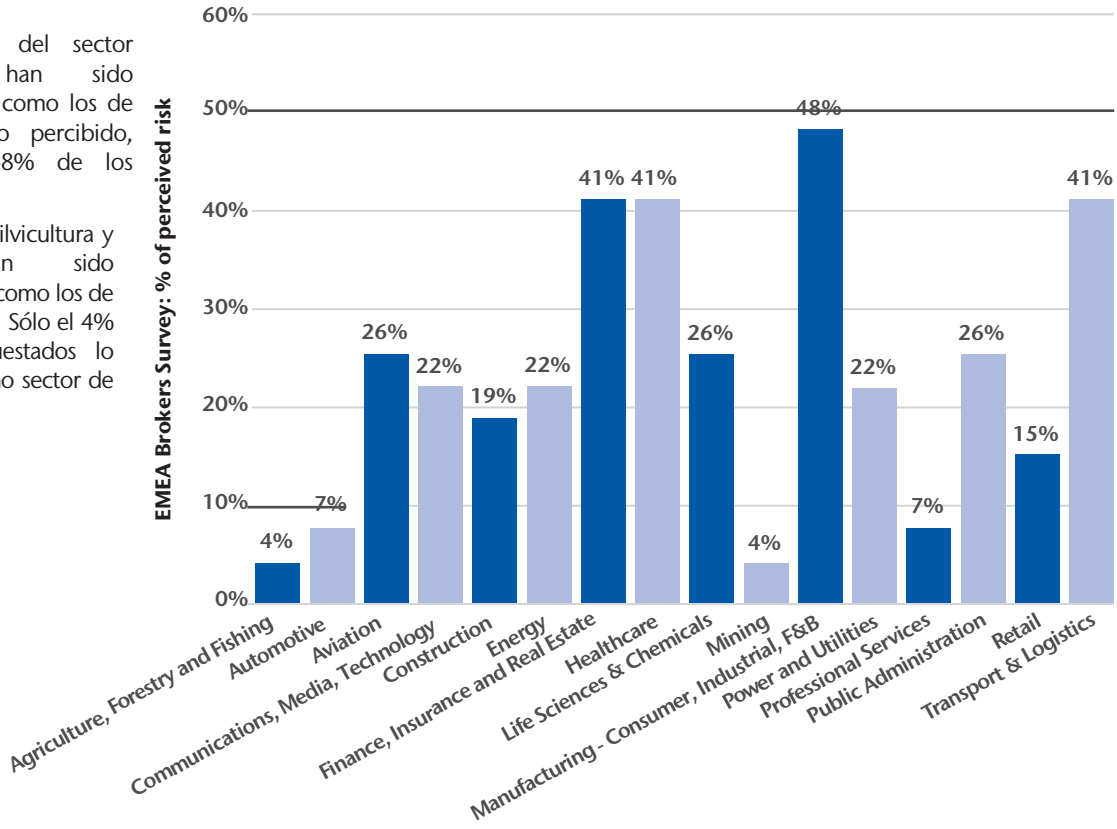


Fuente: Aon EMEA Cyber Carrier Survey Q1 2021

Sectores percibidos con mayor riesgo durante 2021

Comentarios:

- Los clientes del sector industrial han sido identificados como los de mayor riesgo percibido, según el 48% de los encuestados.
- Agricultura, Silvicultura y Pesca han sido identificados como los de menor riesgo. Sólo el 4% de los encuestados lo eligieron como sector de riesgo clave.



Source: Aon EMEA Cyber Broker Survey Q1 2021

Consideraciones a la cobertura

En respuesta a las tendencias de riesgo y siniestralidad descritas anteriormente, los aseguradores están ajustando su enfoque de suscripción, revisando los términos y condiciones de la cobertura y reevaluando el despliegue de la capacidad. Los siguientes son ejemplos específicos de consideraciones de cobertura que los asegurados tendrán en consideración en 2021.

Cobertura de ransomware

Los eventos de ransomware y sus pérdidas asociadas son citados por muchas aseguradoras como un factor importante que impacta en sus ratios de siniestralidad. Si no se proporciona la información de suscripción adecuada, o si la información proporcionada se considera desfavorable, las aseguradoras pueden tratar de limitar su cobertura para las pérdidas por eventos de ransomware:

- Varias aseguradoras están adoptando una estrategia de despliegue de límites en la que pueden limitar el agregado que ofrecen a cualquier asegurado a algún factor del límite total de la póliza.
- Se está proponiendo el co-aseguro (con el asegurado), en algunos casos, junto con un sub-límite.
- Se están revisando los periodos de espera para los acuerdos de seguro de interrupción de la actividad empresarial relacionados con eventos de ransomware, que en algunos casos pueden llegar a ser de 24 horas.
- En los casos más extremos, cuando faltan controles críticos, las aseguradoras pueden tratar de incluir exclusiones de "eventos de ransomware" en las pólizas.

Es fundamental tener en cuenta que, aunque las aseguradoras están utilizando estos enfoques para limitar su exposición, estas restricciones de cobertura no están diseñadas para aplicarse únicamente a un acuerdo de seguro de ransomware o ciberextorsión. Más bien, la restricción está redactada de tal manera que se aplica al ransomware como vector de ataque (un "evento de ransomware"), y por lo tanto puede limitar la cobertura de cualquier pérdida que surja de tal ataque.

Interrupción del negocio

El compromiso de SolarWinds ha hecho que las aseguradoras revisen su exposición global a los riesgos sistémicos, agregados y correlacionados, relacionados con la cadena de suministro de software.

Varias aseguradoras están revisando la amplitud de la cobertura ofrecida para las pérdidas por interrupción de la actividad, con la intención de limitar la exposición financiera a un evento sistémico de las siguientes maneras:

- Reconsideración de los periodos de espera. En muchos casos, los periodos de espera se han negociado entre seis y ocho horas (y en algunos casos se han eliminado por completo).
- El mercado está empezando a presionar para que los periodos de espera se acerquen a las 24 horas, como los que se ven en el mercado inmobiliario.
- Limitación de la exposición al límite agregado. Esto se está consiguiendo mediante la reintroducción de sublímites o la exigencia de coaseguro.

Proveedores de Primera Respuesta

A medida que los índices de siniestralidad se deterioran, las aseguradoras están revisando de cerca los costes de los proveedores de terceros en los que se incurre para investigar y responder a los incidentes cibernéticos.

Para reducir (o al menos combatir el aumento de) estos costes, las aseguradoras están demostrando menos flexibilidad en el uso de proveedores no pertenecientes al panel o preacordados.

Además de que hay más desafíos relacionados con el uso de proveedores no pertenecientes a un panel -en particular si no hubo discusión/vigilancia del proveedor antes de su contratación para un incidente- las aseguradoras están haciendo menos excepciones relacionadas con las tarifas de los proveedores.

Cada vez es más frecuente que las aseguradoras sólo reembolsen una cantidad igual a la que la aseguradora habría pagado a un proveedor de panel.

Cómo mejorar el riesgo – Recomendaciones

Con el cambio a un mercado de ciberseguro duro a finales de 2020, es fundamental un enfoque de intermediación estratégico basado en el riesgo. La preparación de la presentación de la suscripción es clave para diferenciar a nuestros compradores de seguros Cyber en el mercado y para mantener el acceso a la capacidad. Comenzar el proceso de colocación (renovación) con antelación, no sólo invirtiendo tiempo en la calidad de la preparación de la presentación de la suscripción, sino también reuniéndose con los suscriptores clave, centrándose en las relaciones existentes con las aseguradoras y determinando el apetito actual (de renovación) puede mitigar las sorpresas.

Focus on: Cyber Security

Aunque ninguna organización puede eliminar la amenaza de una brecha, es fundamental poder demostrar los pasos básicos para reducir el riesgo y disminuir significativamente el impacto de la amenaza. Esto requiere estrategias proactivas de mitigación de riesgos que incluyan la evaluación, las pruebas y la mejora de las prácticas. También requiere una preparación para la respuesta a incidentes, incluyendo la realización de ciber ejercicios y la contratación proactiva de proveedores clave de respuesta a incidentes. Aprovechar los recursos disponibles a través de los aseguradores puede mejorar el resultado en caso de que se produzca una pérdida. Por ejemplo, tras las recientes vulnerabilidades de Microsoft Exchange, las aseguradoras cibernéticas están preguntando si las organizaciones utilizan Microsoft Exchange, y si han realizado una evaluación de compromiso.

Focus on: Ransomware & Business Interruption

Dado que las aseguradoras están observando un aumento de la frecuencia y la gravedad de las pérdidas relacionadas con el ransomware, las empresas deben estar preparadas para demostrar que están preparadas para un ataque. Las aseguradoras están revisando esta exposición a través de cuestionarios complementarios específicos y el uso de tecnología de escaneo. La atención se centra en la planificación de la continuidad del negocio/recuperación de desastres, los controles de acceso privilegiado, la autenticación multifactorial, el escaneo/prueba proactiva y la preparación general de la respuesta a incidentes. Este vector de ataque es de máxima preocupación para los suscriptores y seguirá transformando el mercado de los seguros durante los próximos años.

Focus on: Privacy

La madurez en materia de privacidad puede demostrarse mediante políticas establecidas y actualizadas que aborden los contratos con terceros, la presencia on line, los proveedores de servicios, las cadenas de suministro y cada unidad de negocio. Las nuevas normativas y requisitos en materia de privacidad deben revisarse de forma rutinaria con los asesores, y el lenguaje de los seguros debe revisarse para garantizar que es lo suficientemente amplio como para responder a la evolución del entorno.

Focus on: Cyber Security Culture

La formación en ciberseguridad y phishing de los empleados puede demostrar una cultura de ciberseguridad. Ya no se trata sólo de un problema de Administración/Informática/Finanzas, los empleados deben recibir formación para trabajar en la lucha contra los actores maliciosos y reducir las vulnerabilidades comunes. Si no demuestran una formación adecuada en materia de seguridad, las aseguradoras pueden tener dificultades para ofrecer condiciones de cobertura o primas competitivas.

Focus on: Contracts

Los contratos de terceros son de consideración desde el punto de vista de la cadena de suministro de tecnología y los negocios contingentes/dependientes. Teniendo en cuenta el compromiso de SolarWinds, estos proveedores críticos de la cadena de suministro y de TI corren un mayor riesgo de sufrir ataques de “single point of failure" que afecten a múltiples organizaciones. Es fundamental comprender cómo responden tanto los contratos como los seguros en caso de una violación de la seguridad de la cadena de suministro.

Focus on: Insurer Transparency and Communication

A medida que los riesgos ciber crecen en complejidad, es importante no sólo asegurar el compromiso del asegurador del Primario en relación con los términos y condiciones de la cobertura, sino también asegurar que el asegurador del exceso entienda las disposiciones de la póliza primaria. Además, es prudente revisar las exclusiones que podrían provenir de otros ramos de seguros como el de Fraude, TRDM, Accidentes y Responsabilidad Civil. Mantener una relación clara y transparente tanto con las aseguradoras de las capas Primarias como con las de los Excesos puede mejorar la tramitación de los siniestros.

Contacts

Vanessa Leemans
Chief Broking Officer
Cyber Solutions EMEA
vanessa.leemans@aon.co.uk

Alistair Clarke
Cyber Insurance Leader
Global Broking Centre
alistair.clarke@aon.co.uk

Naomi Cresswell
Cyber Insurance Leader
United Kingdom
naomi.cresswell10@aon.co.uk

Duane Folkard
Cyber Insurance Leader
United Kingdom
duane.folkard@aon.co.uk

Søren Carl Stryger
Cyber Insurance Leader
Nordics
soren.stryger@aon.dk

Marie-Louise de Smit
Cyber Insurance Leader
Netherlands
marie-louise.de.smit@aon.nl

Thomas Pache
Cyber Insurance Leader
DACH
thomas.pache@aon.de

Marion Rollandy-Claret
Cyber Insurance Leader
Switzerland
marion.rollandy-claret@aon.com

Vincenzo Aliotta
Cyber Insurance Leader
Italy
Vincenzo.Aliotta@aon.it

Claudia Beatriz Gomez
Cyber Insurance Leader
Spain
claudiabeatriz.gomez@aon.es

David Molony
Cyber Risk Leader
Cyber Solutions EMEA
david.molony@aon.co.uk

Alex Hornsby
Senior Cyber Risk Consultant
Cyber Solutions EMEA
alex.hornsby@aon.co.uk

Karl Curran
Cyber Insurance Leader
Ireland
Karl.Curran@aon.ie

Stéfanie Deley
Cyber Insurance Leader
Belgium
stefanie.deley@aon.com

Marcos Oliveira
Cyber Insurance Leader
Portugal
marcos.menezes.oliveira@aon.pt

John Papageorgiou
Cyber Insurance Leader
Greece
john.papageorgiou@aon.gr

Gizem Polat
Cyber Insurance Leader
Turkey
gizem.guldursun@aon.com.tr

Eddie Aviad
Cyber Insurance Leader
Israel
Eddie@aon-israel.com

Thomas Powell
Cyber Insurance Leader
Middle East
thomas.powell@aon.ae

Zamani Ngidi
Cyber Insurance Leader
South Africa
zamani.ngidi2@aon.co.za

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber security, risk and insurance management, investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance. For further information on our capabilities and to learn how we empower results for clients, please visit : http: //aon.mediaroon.com

aon.com/cyber-solutions

Empower Results®