Seguro Cibernético – la amenaza y/o la oportunidad del futuro ?

Convención AMIS 6-7.5.2015

Maximilian Kückemanns

Munich RE

Seguro Cibernético – la amenaza y/o la oportunidad del futuro ?

Munich RE

Agenda

Pérdidas Cibernéticas – ¡la amenaza!

Seguro Cibernético – ¡convirtiendo la amenaza en oportunidades!

Seguro Cibernético – ¿a qué se refiere?

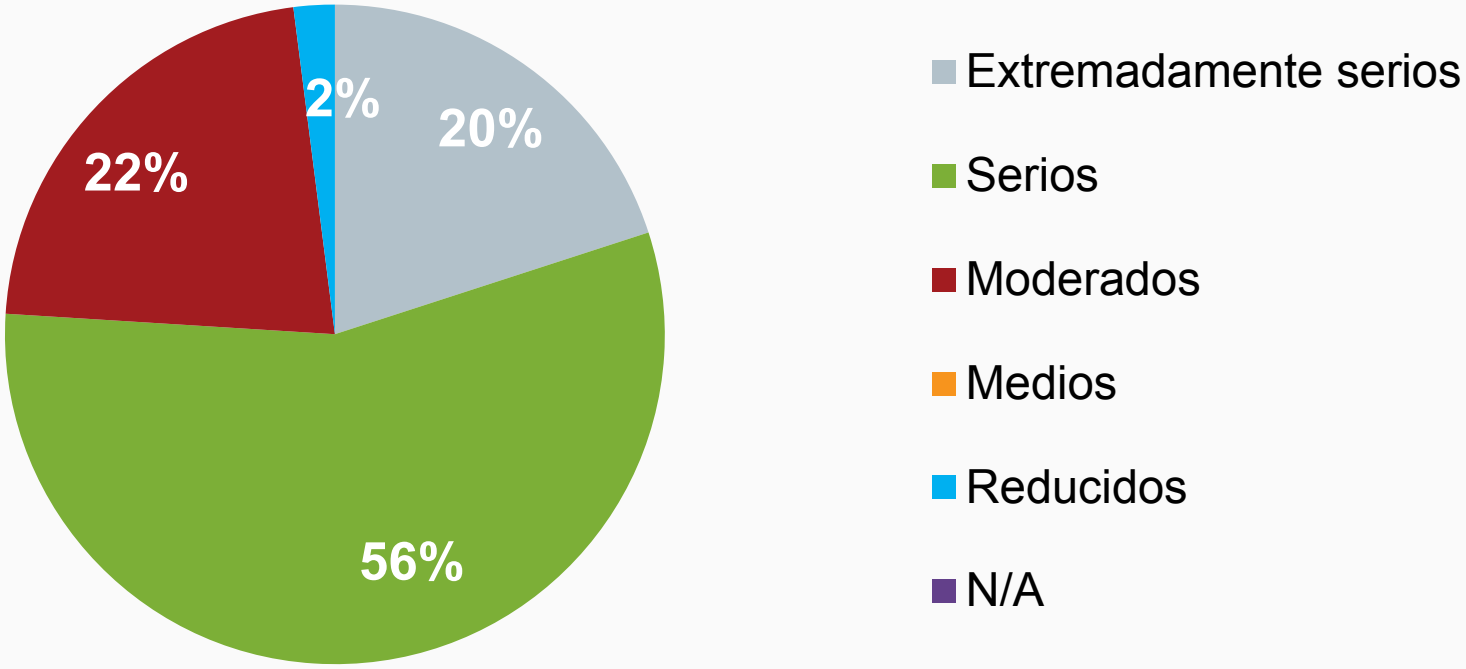
Riesgos Cibernéticos – ¿cómo encaja en su mercado?

Reaseguro – ¿cómo podemos ayudarles?

Los riesgos cibernéticos son percibidos cada vez más como una seria amenaza

Munich RE

¿Cómo valoraría usted los peligros potenciales en su organización derivados de riesgos cibernéticos?



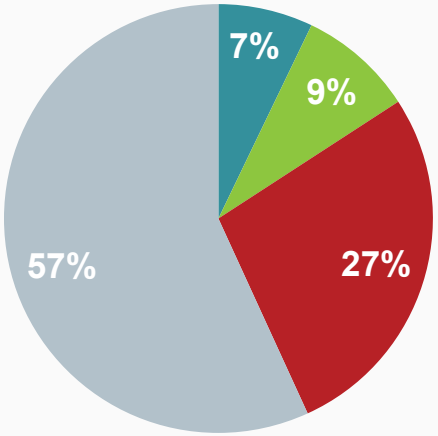
Fuente: 2014 Network Security & Cyber Risk Management by Advisen Ltd. & Zurich – con encuestados principalmente europeos

Elevados costos por *Data Breach*

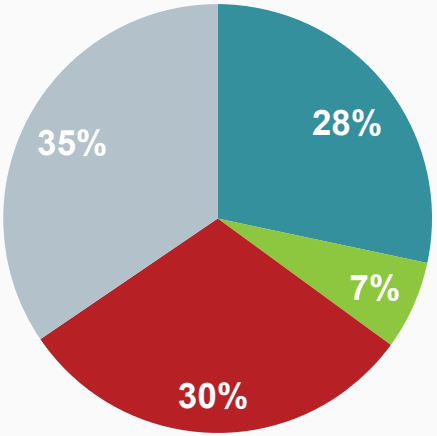
Munich RE

2014: Coste total promedio de la fuga de datos por organización

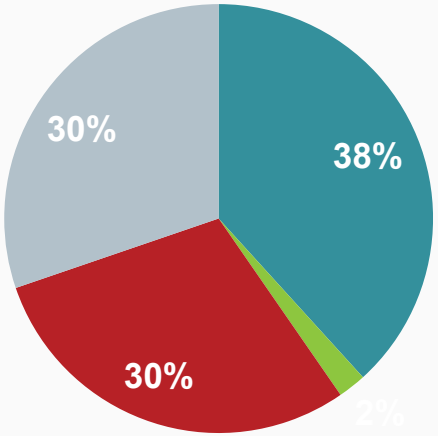
USA ($ 5,85m)



Alemania ($ 4,74m)



Australia ($ 2,59m)



- Detección y generalización
- Costes de notificación
- Costes post *Data Breach*
- Pérdida de negocio

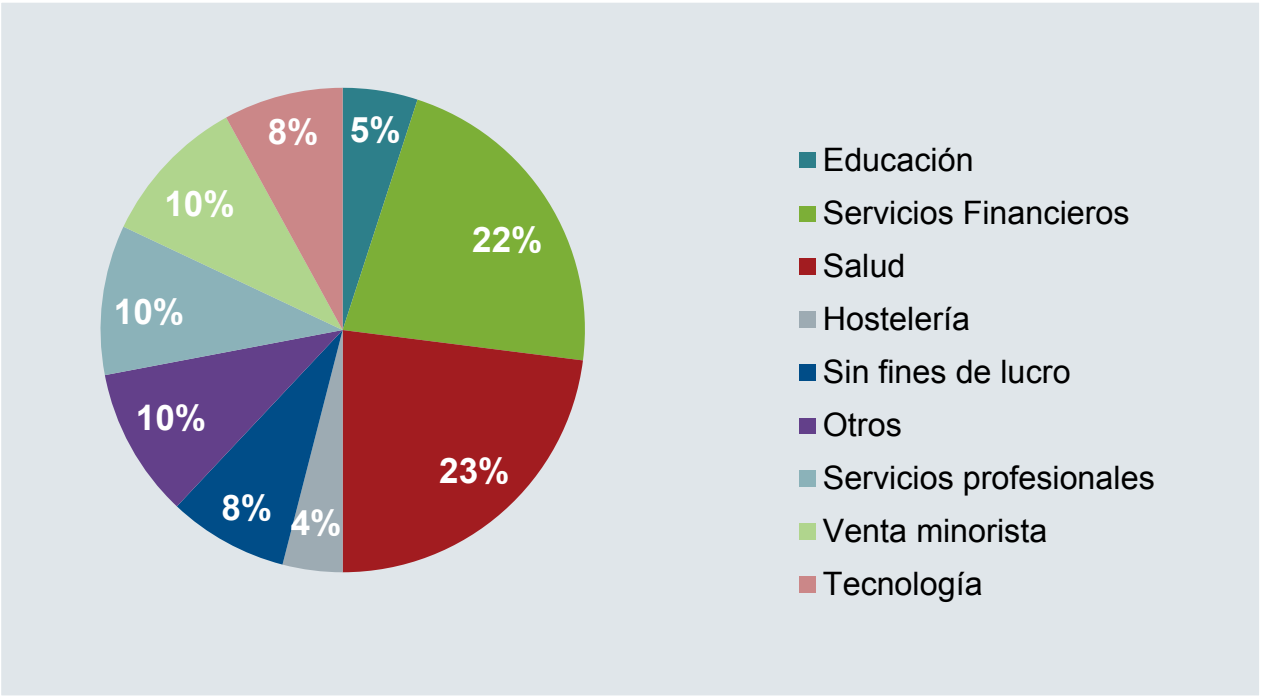
Los componentes del coste de un *Data Breach* varían significativamente entre países

Fuente: Ponemon 2014 Cost of Data Breach Study

Elevados costos por *Data Breach* por sector

Munich RE

Porcentaje promedio de *Data Breach* por sector de negocios



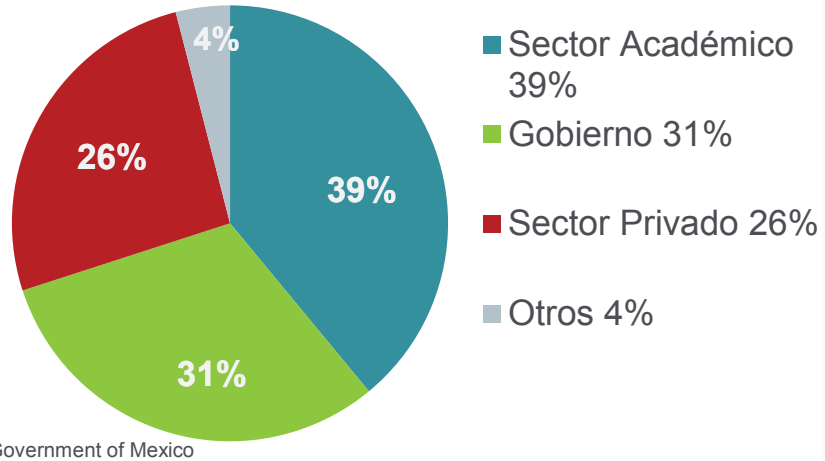
Salud y Servicios Financieros son los sectores más afectados

Fuente: Netdiligence 2014 Cyber Claims Study

Casos de responsabilidad debido al delito cibernético en México

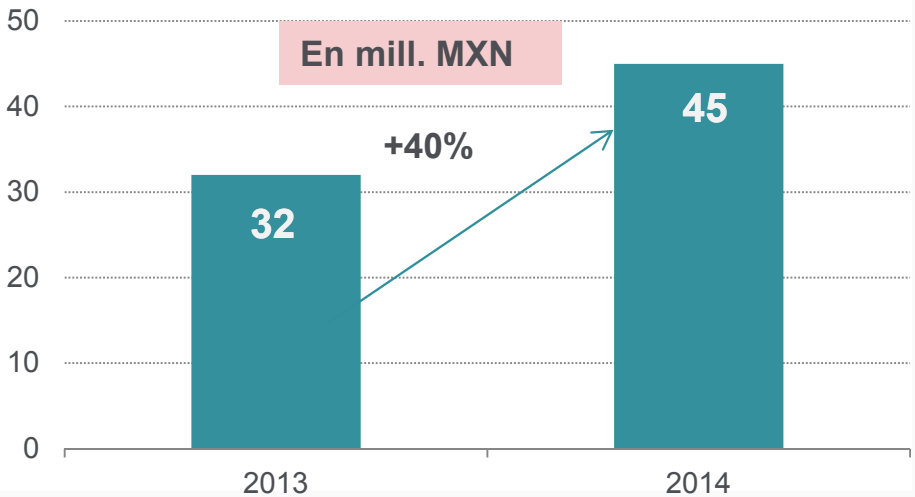
Munich RE

Entidades Afectadas por Delitos Cibernéticos



Source: Government of Mexico

Incremento de Costos debido al Delito Cibernético



Fuente: Policía Federal de México

Casos Reales en México

- Filtraron datos de 3,000 empleados de Telcel.
- Robaron datos de 80,000 clientes de Subay.
- Robaron datos de 1,5 millones de Tarjetas de Crédito.
- Anonymous asegura haber robado datos de 700,000 usuarios de Televisa.
- “Hackean” sitio del Tribunal Electoral de Puebla.
- Uso de un ransomware disfrazado como “Anti-Child Porn Spam Protection”. El delincuente tuvo acceso a las computadoras de sus objetivos, instaló el malware, bloqueó el acceso de los propietarios y exigía tres mil dólares para recuperar los archivos.

→ **En el 2014, el costo de delitos cibernéticos llegó a mas de $40 mil millones de Mxn, de acuerdo con un reporte de la empresa de seguridad cibernética Norton.**

Seguro Cibernético– la amenaza y la oportunidad del futuro

Munich RE

Agenda

Pérdidas Cibernéticas – ¡la amenaza!

Seguro Cibernético – ¡convirtiendo la amenaza en oportunidades!

Seguro Cibernético – ¿a qué se refiere?

Riesgos Cibernéticos– ¿cómo encaja en su mercado?

Reaseguro – ¿cómo podemos ayudarles?

Amenazas cibernéticas existentes pueden transformarse en oportunidades de negocio

Munich RE

"TJX se enfrentó al robo de la información de 45,7 millones de tarjetas de crédito, por medio de "war driving""

+ 144%

Incremento en el número de ataques cibernéticos exitosos sobre negocios a todas las escalas (2010-2014)

¡Convertir la amenaza en oportunidades!

-

Cibernético supone un potencial de negocio para las cías. aseguradoras

+221%

Incremento del tiempo medio para resolver incidentes (2010-2014)

"Home Depot admite que 53 millones de direcciones e-mail y los datos de 56 millones de tarjetas de crédito han sido robados en Data Breach"

"JP Morgan sufre Data Breach sobre 76 millones de clientes privados y sobre 7 millones de clientes corporativos"

+ 95%

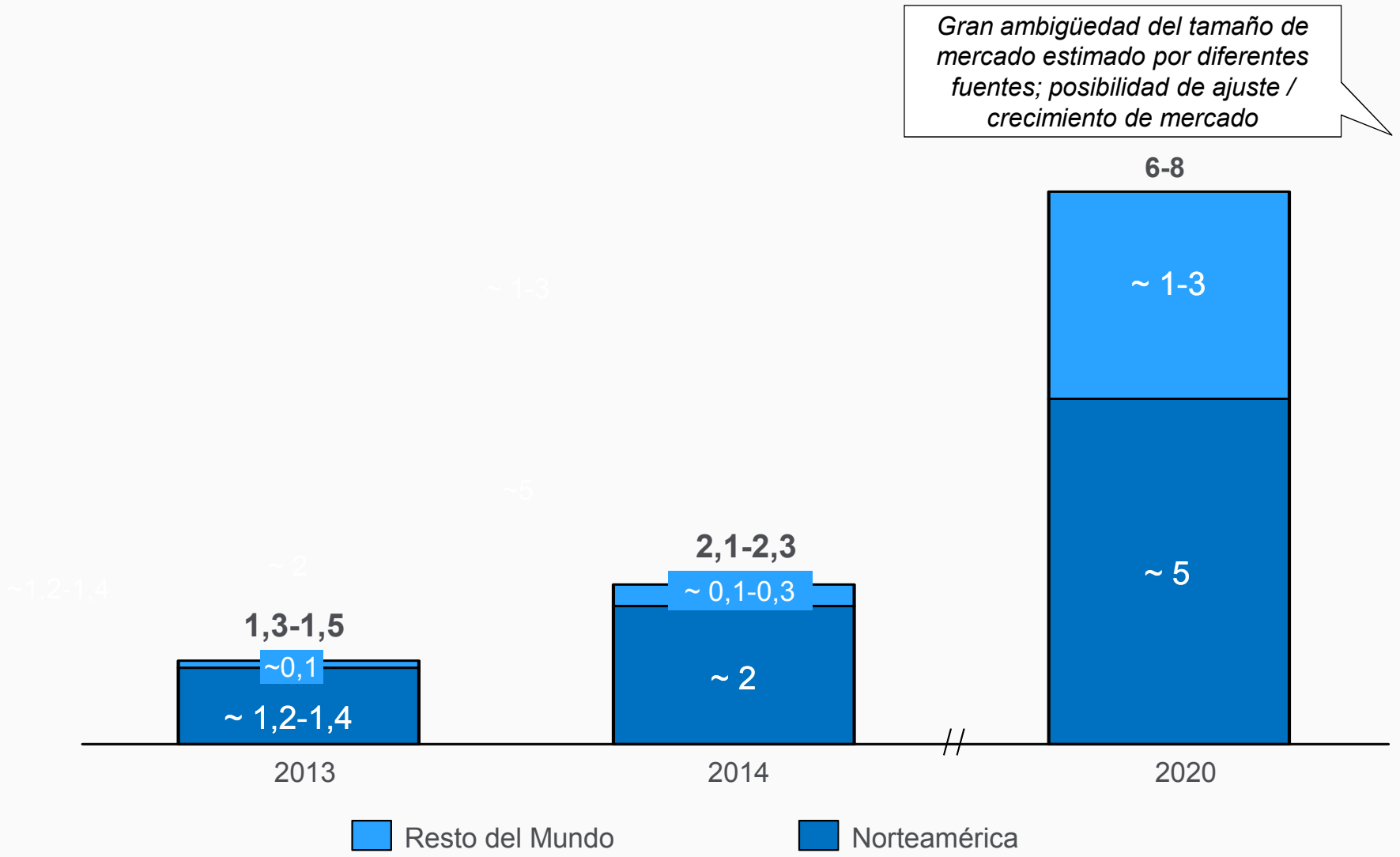
Incremento del costo del crimen Cibernético por compañía (2010-2014)

Fuente: 2015 CYREN Cyberthreat yearbook; IT Governance

Fuerte crecimiento esperado del Seguro Cibernético – en Norteamérica, así como en el resto del Mundo

Munich RE

Prima Estimada - Mercado se Seguro Cibernético Primario (2013, 2014 & 2020, en USD bn.)



Fuente: estimaciones Munich Re, basadas en diferentes fuentes externas (Marsh & McLennan, Advisen, Barbican Insurance, Allianz)

¿Está usted en la situación de realizar el potencial de negocio adicional en América Latina?

Munich RE

Y nuestro mercado?

Aseguradoras globales están preparadas para introducir sus productos cibernéticos en América Latina

Incremento en la demanda lleva a un incremento significativo del negocio y la prima potencial

Ejemplos recientes de pérdidas prominentes llevan a un incremento mundial en la demanda de coberturas Cibernéticas

Fuente: Munich Re

Seguro Cibernético – la amenaza y/o la oportunidad del futuro ?

Munich RE

Agenda

Pérdidas Cibernéticas – la amenaza!

Seguro Cibernético – convirtiendo la amenaza en oportunidades!

Seguro Cibernético – ¿a qué se refiere?

Riesgos Cibernéticos – ¿cómo encaja en su mercado?

Reaseguro – ¿cómo podemos ayudarles?

Normalmente el seguro Cibernético incluye cobertura de 1ª y 3ª parte para una amplia variedad de escenarios de pérdida

Munich RE

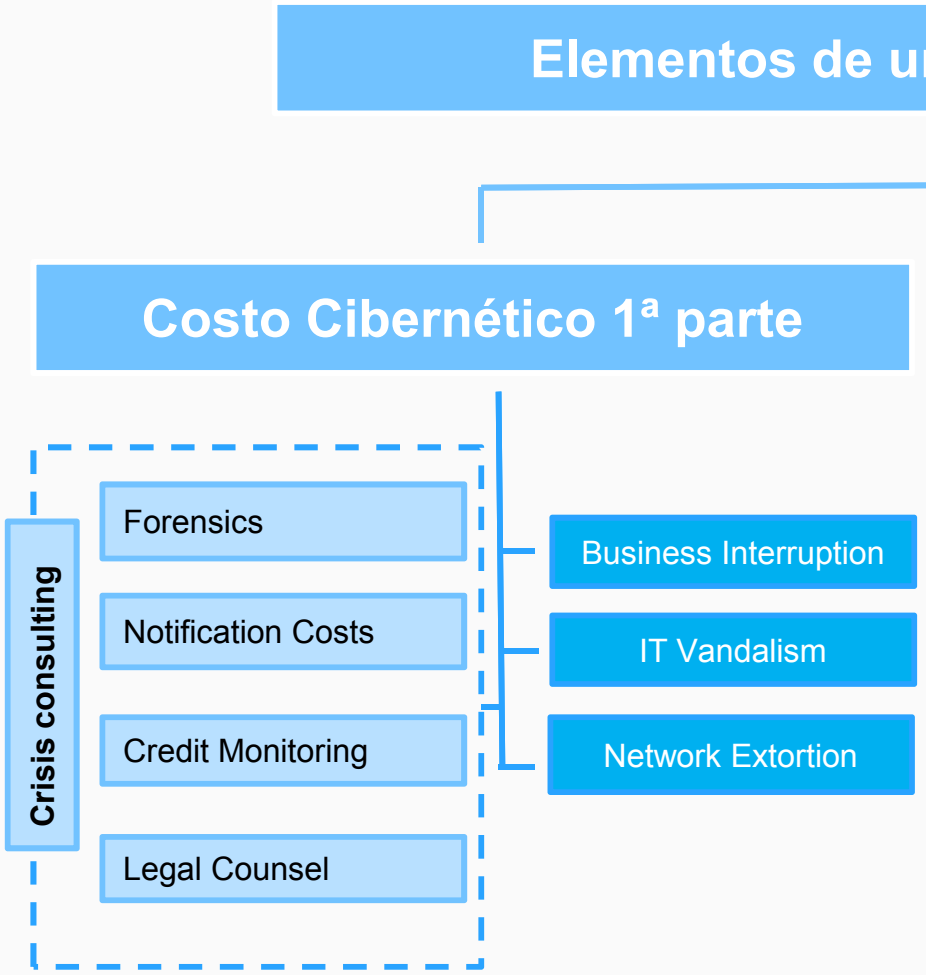
- ***"Cyber Liability"*** normalmente cubre aspectos de1ª **y** 3ª parte.
- Hay muchas pólizas de seguro cibernético disponibles con diferentes nombres como *Privacy Protection, Data Security, Cyber Liability, Tech E&O, Media Liability etc.*
- La cobertura depende de la necesidades individuales del asegurado.
- Diferente combinación de elementos según compañías y sectores de industria.
- Diferentes sub-límites pueden aplicarse a las diferentes coberturas posibles.

Causas que motivan una póliza cibernética pueden ser:

- Virus
- Ataque Hacker
- Acto pernicioso por parte de empleado/contratado
- Error Humano (e.g. descuido en el tratamiento de datos)
- Error de Software

Fuente: Munich Re

Crisis consulting es el elemento principal de la cobertura 1ª parte en los EEUU



Crisis Consulting: pagos a profesionales por acciones para prevenir, mitigar o restaurar los efectos potencialmente adversos de un siniestro

Business Interruption: ingresos del negocio no recibidos como resultado de la interrupción o no funcionamiento de la red de servicios operativos debido a un ataque fraudulento sobre la red informática del asegurado.

IT Vandalism: costes incurridos directamente por alteración, corrupción, daño, pérdida o destrucción de ciertos datos, ante la necesidad de recuperarlos o repararlos.

Network Extortion: pagos por extorsión en que un asegurado incurre, resultado directo de una amenaza criminal en cuanto a publicar información sensible o inutilizar una red informática.

Fuente: Munich Re

Cobertura de 3ª parte incluye una amplia variedad de coberturas de responsabilidad civil

Munich RE

Elementos de una póliza Cibernética

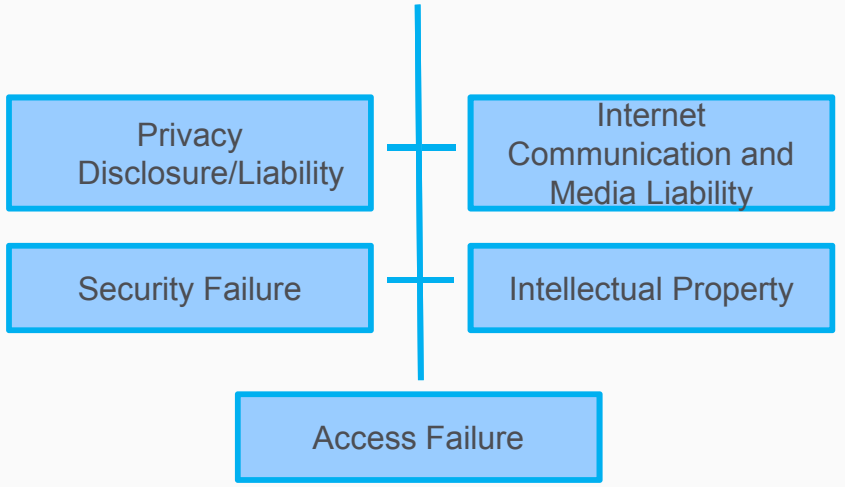
Privacy Disclosure/Liability: Acceso no autorizado, liberación o transmisión de información personal sensible debido al fallo para proteger tal información o publicación por parte de un empleado

Security Failure: Cualquier daño por acceso no autorizado a la red, transmisión de virus, etc. debido a un fallo de seguridad en el sistema del asegurado.

Internet Communication and Media Liability: Daño en la reputación de una 3ª parte como e.g. injurias y calumnias hacia personas o productos por medio de publicación falsa de cualquier contenido electrónico o en medios digitales.

Intellectual Property: cualquier infracción sobre el contenido protegido por propiedad intelectual debido al fallo en la protección adecuada de tal información

Access Failure: sistemas no disponibles por acceso denegado o dañado a los datos de una 3ª parte (cliente) debido a un fallo en el sistema de seguridad de la red informática



Fuente: Munich Re

Consideraciones importantes para la suscripción y el manejo de siniestros

Munich RE

Consideraciones de suscripción

- Las **leyes de protección de datos** de cada país tienen un impacto en la necesidad general y los elementos de cobertura para protecciones cibernéticas
- Sin embargo, la **residencia del reclamante** decide a cuál ley de protección de datos tiene que adherirse en caso de una reclamación → **la Web no tiene fronteras**
- **Implicaciones en la evaluación de riesgos:**
  - ¿Representación del asegurado en otros países?
  - Cantidad y tipo de datos extranjeros en la base de datos del asegurado?
  - ¿Medidas de seguridad cibernética tomadas por el asegurado? (HW/SW, procesos, capacitación de empleados, etc.)
  - ¿Fuente externa de datos y servicios?

Manejo de siniestros

- La **acción inmediata** en caso de una reclamación puede reducir significativamente su impacto

  → cooperación con expertos externos requeridos
- **Experiencia jurídica y reglamentaria** para entender los requisitos normativos y para valorar pronto el potencial de las reclamaciones, diseñar contramedidas y defender reclamaciones
- **Investigaciones forenses** con respecto a la causa y extensión del incidente
- Evaluación de **mejoras requeridas al sistema/a la seguridad**
- **Verificación de crédito** y **notificación** puntual **de los clientes** de acuerdo con el reglamento
- **Apoyo con respecto al daño de reputación** (estrategia de comunicación, manejo de medios de comunicación)

Seguro Cibernetico – la amenaza y/o la oportunidad del futuro ?

Munich RE

Agenda

Pérdidas Cibernéticas – la amenaza!

Seguro Cibernético – convirtiendo la amenaza en oportunidades!

Seguro Cibernético – ¿a qué se refiere?

Riesgos Cibernéticos – ¿cómo encaja en su mercado?

Reaseguro – ¿cómo podemos ayudarles?

La situación legal específica de mercado es el primer determinante de la demanda Cibernética para *Data Breach*

Munich RE

Situación legal específica de mercado, principal determinante de la responsabilidad cibernética y la demanda de protección

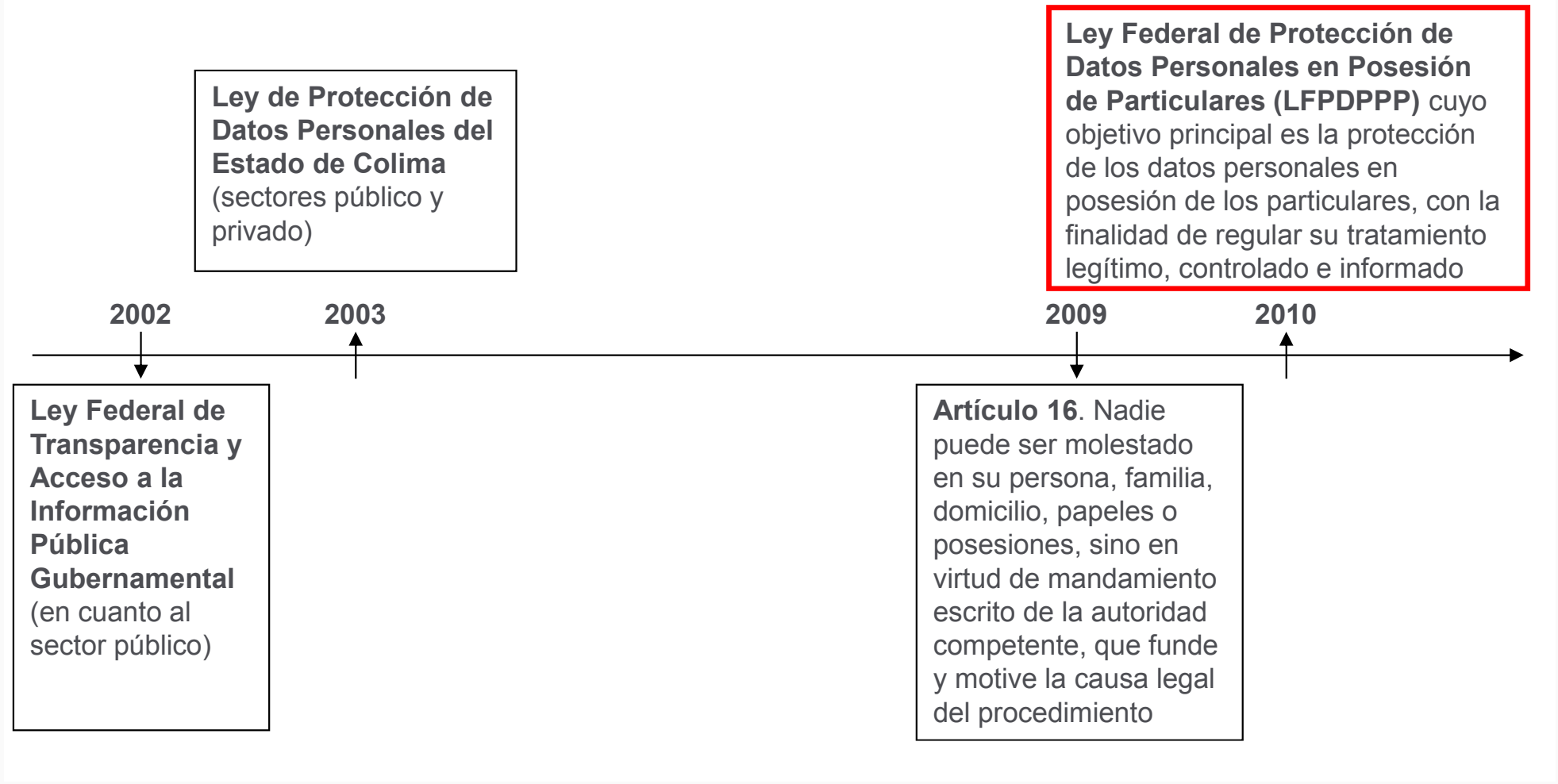
- ¿Existen leyes con respecto a protección de datos?
- ¿Define la jurisdicción local los datos como una propiedad tangible?
  → Si es así, los datos se cubren bajo property, de otro modo se requiere protección cibernética.
- ¿Qué tipo de datos se define merecen ser protegidos?
  → Para este tipo de datos, las compañías pueden resultar responsables en el caso de pérdidas de datos potenciales (normalmente información personal identificable (PII en inglés) e información médica protegida (PHI));
- ¿Determina la legislación acciones requeridas en caso de *data breach* / pérdida potencial de datos?
- ¿Determina la legislación local ciertos estándares de gestión del riesgo para compañías o industrial?(e.g. estándares de seguridad de la industria de pago con tarjetas etc.)?
- ¿Existen autoridades locales que reúnen información, e.g. de delitos ciberneticos?

Fuente: Munich Re

Desarrollo de situación legal en cuanto al riesgo cibernético en México

Munich RE

Línea Cronológica



Situación actual del seguro cibernético en México

Munich RE

Perspectivas

- La Ley de Protección de Datos de México requiere que los datos estén sujetos a ser notificados de violaciones si la violación afecta significativamente sus derechos económicos o morales.
- El Seguro de Riesgos Cibernéticos es relativamente nuevo en México.
- Cada vez es más común ver reportes de multas contra compañías por violar las leyes de privacidad mexicanas - esto puede aumentar el interés en las pólizas de seguro cibernético.
- De acuerdo con la Policía Federal, hubo un aumento del 113% en incidentes de seguridad cibernética en el 2013 en comparación con el 2012 en México.

Desafíos

- El mercado de Seguros prevén los riesgos que enfrentan de forma limitada y algunas veces se considera que están cubiertos por las pólizas existentes.
- Sólo algunas aseguradoras están ofreciendo pólizas, como una póliza específica o como un endoso.
- Mejorar la situación a nivel país para enfrentar una amenaza cibernética.

Seguro Cibernetico – la amenaza y/o la oportunidad del futuro ?

Munich RE

Agenda

Pérdidas Cibernéticas – la amenaza!

Seguro Cibernético – convirtiendo la amenaza en oportunidades!

Seguro Cibernético – ¿a qué se refiere?

Riesgos Cibernéticos – ¿cómo encaja en su mercado?

Reaseguro – ¿cómo podemos ayudarles?

Posibles próximos pasos dependiendo de la posición estratégica respecto a seguro cibernetico

Munich RE

¿Dónde ven ustedes prioridades estratégicas con respecto a seguro Cibernético hacia el futuro?

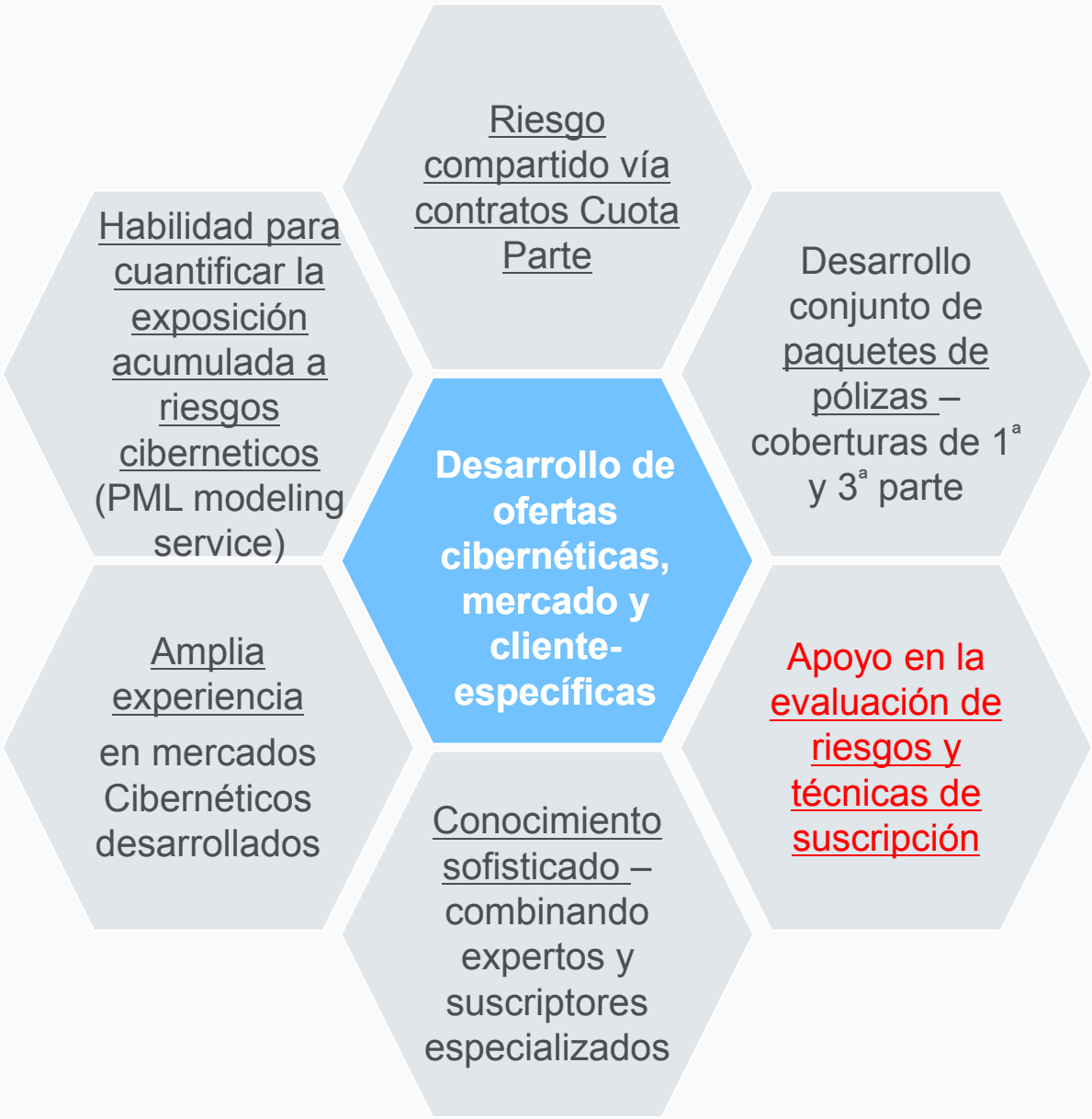
¿Cómo valorarían su propia exposición a riesgos cibernéticos y con qué medidas cuentan o consideran contar para gestionar esta exposición?

¿Cuál es su perspectiva sobre una posible cooperación en cuanto a seguro cibernético?

¿Qué contribuciones específicas esperan que puede ofrecer el mercado de reaseguro?

Apoyo en el desarrollo de productos
Desde la perspectiva del reasegurador

Munich RE



Fuente: Munich Re

Take aways

Munich RE

1	Los riesgos Cibernéticos afectan a todos, no hay un sector que no tenga alguna exposición.
2	Es un negocio para desarrollar mas ampliamente en México y la región (?)
3	Las áreas de suscripción y siniestros tienen que colaborar juntos de forma muy efectiva.
4	La definición de coberturas de 1ª y ·3ª parte es muy importante.
5	Estrecha colaboración entre la Aseguradora y el Reasegurador.

Munich RE

NOT IF, BUT HOW !

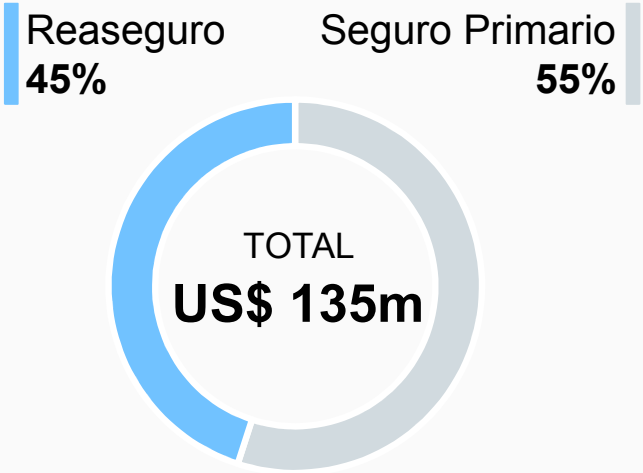
Munich Re cuenta con una amplia experiencia – tanto del lado del reaseguro como del seguro primario

Munich RE

Reaseguro

First mover
y líder de mercado

- Más de 10 años de experiencia reasegurando carteras cibernéticas y grandes riesgos
- Sofisticados modelos de acumulación de riesgos (e.g. virus, cloud, critical infrastructure)
- Cooperación conjunta con cedentes (e.g. desarrollo de productos en mercados cibernéticos menos desarrollados)



Seguro primario

Tomador especializado de *single-risk* en una amplia gama de riesgos ciberneticos

- **Hartford Steam Boiler**
  Market player establecido en USA para responsabilidad cibernetica y coberturas de privacidad sobre PYMEs y particulares
- **Corporate Insurance Partner**
  Soluciones específicas tanto por industria como personalizadas para grandes clientes; amplia variedad de coberturas y límites superiores a la media

Fuente: Munich Re

TJX se enfrentó al robo de 45,7 millones de credenciales de tarjetas de crédito mediante “war driving”

Munich RE

TJX *Data breach* – uno de las pérdidas más famosas y caras

- Desde Julio de 2005 hasta Enero de 2007 el minorista TJX se enfrentó al robo de 47,5 millones de credenciales de tarjetas de crédido mediante “war driving”.
- Al tiempo del robo TJX tenía un certificado válido de PCI-DSS (Payment Card Industry Data Security Standard). Se reconoció retroactivamente que 9 de estos 12 criterios de seguridad no fueron cumplidos.
- Consumidor, accionista, bancos e instituciones de tarjetas de crédito instaron a la compañía a compensar los daños causados por la pérdida de negocio, además de indemnizaciones.
- Las acciones con clientes incluyeron 3 años de monitorización del crédito, seguro para la el robo de identidad y la compensación de costes.
- Las acciones con los bancos, entidades de tarjetas de crédito y el Estado acumularon un pago de 75 millones de USD
- TJX aceptó tras el incidente una auditoría annual de la seguridad estipuladad por FTC durante un periodo de 20 años

Source: Munich Re

El comportamiento negligente de un empleado puede causar más de 114 millones de USD de pérdidas

Munich RE

El *Data breach* de CBR Systems

- La compañía afectada fue CBR Systems Inv., que afirma ser el mayor y más puntero banco de células madre a nivel mundial.
- Un empleado tomó copias de seguridad, un ordenador portátil, un disco duro extraíble, un dispositivo USB y otros objetos para transportarlos de una oficina cercana a las oficinas centrales.
- Los dispositivos, que contenían información desencriptada de casi 300.000 personas, fueron robados del coche del empleado
- Los datos robados incluían nombres, género, número de seguro social, número del carnet de conducir, número de tarjetas de crédito y débito y pasaporte, utilizados para acceder a la red informática de CBR
- Se interpuso una demanda colectiva y la indemnización final alcanzó los 114 millones de USD, por costes y gastos del demandante.
- Considerando el número de records, el coste medio por archivo suma 285 dólares.

Source: Munich Re

Las terminales de venta muestran ser vulnerables a virus informáticos – con dramáticas consecuencias

Munich RE

The Target Data Breach 2013

- Desde el 27 de Noviembre al 15 de Diciembre de 2015, un virus informático infectó las terminales de venta de la empresa Target, afectando a 1.797 tiendas en los EE.UU.
- Información de tarjetas de crédito y débito de cerca de 40 millones y PII de 70 millones de clientes podrían haber sido revelados por error.
- El hacker trató de vender la información en masa (a precios de entre 20-100 USD cada uno) en el mercado negro a gente que utiliza la información para crear tarjetas falsificadas.
- Los hackers utilizaron un sistema construido para este efecto (RAM memory scraping malware) dirigiéndose a la información que era más vulnerable: la memoria de los datafonos. Tras pasar la tarjeta por el datafono, la información de la tarjeta permanece en la memoria del dispositivo antes de transferirse a un disco duro donde es – según PCI DSS – encriptada.
- La pérdida total se estima cerca de mil millones de USD, incluyendo reembolso a los bancos por re-emitir millones de tarjetas, multas por marcas de tarjetas por no cumplir con las normas PCI, servicios de notificación al cliente, costes legales y monitorización del crédito para millones de usuarios. Adicionalmente costes incurridos por la mejora de la seguridad informática y por la interrupción del negocio.

Source: Munich Re

Escenarios de acumulación crean la necesidad acuciante de gestión y protección del riesgo

Munich RE

„Global Outage of the internet“

- Infección a escala mundial
- Interrupción de gran cantidad de servicios
- Sin prevención posible por el asegurado

No puede (re-)asegurarse

Virus informático auto-reproductivo

- Infección a escala mundial
- Gran número de sistemas afectados en un evento

Modelo de propagación de un “Super Virus”

Gran suministrador de *Cloud Services*

- La acumulación es causada por el efecto de una sola compañía
- Gran cantidad de clientes afectados en un evento

Controlar la exposición según suministrador(-es) de servicios

Fuente: Munich Re