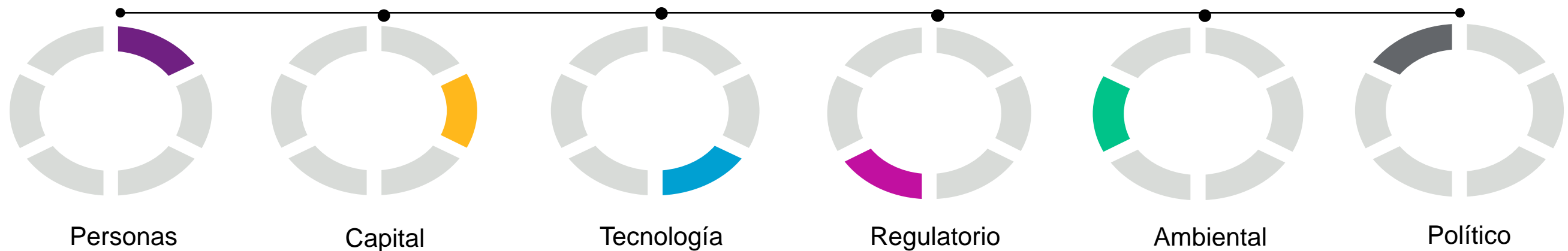


La Evolución del Riesgo Cibernético y el Papel del Seguro



Intersección de Riesgos Cibernéticos

El Riesgo Cibernético es tan impactante porque se encuentra en la intersección entre el riesgo de personas, el riesgo de capital, el riesgo regulatorio, el riesgo de tecnología, el riesgo político y el riesgo ambiental — por lo tanto es muy difícil **cuantificar** y **mitigar**.



Los 5 principales riesgos mundiales en términos de probabilidad, según el reporte de Riesgos Globales del WEF

	2017	2018
1	Eventos Climáticos Extremos	Eventos Climáticos Extremos
2	Migración involuntaria a gran escala	Desastres Naturales
3	Desastres Naturales	Ciberataques
4	Ataques terroristas a gran escala	Fraude o robo de datos
5	Incidente masivo de fraude/ robo de datos	Fracaso de la Mitigación y adaptación al cambio climático

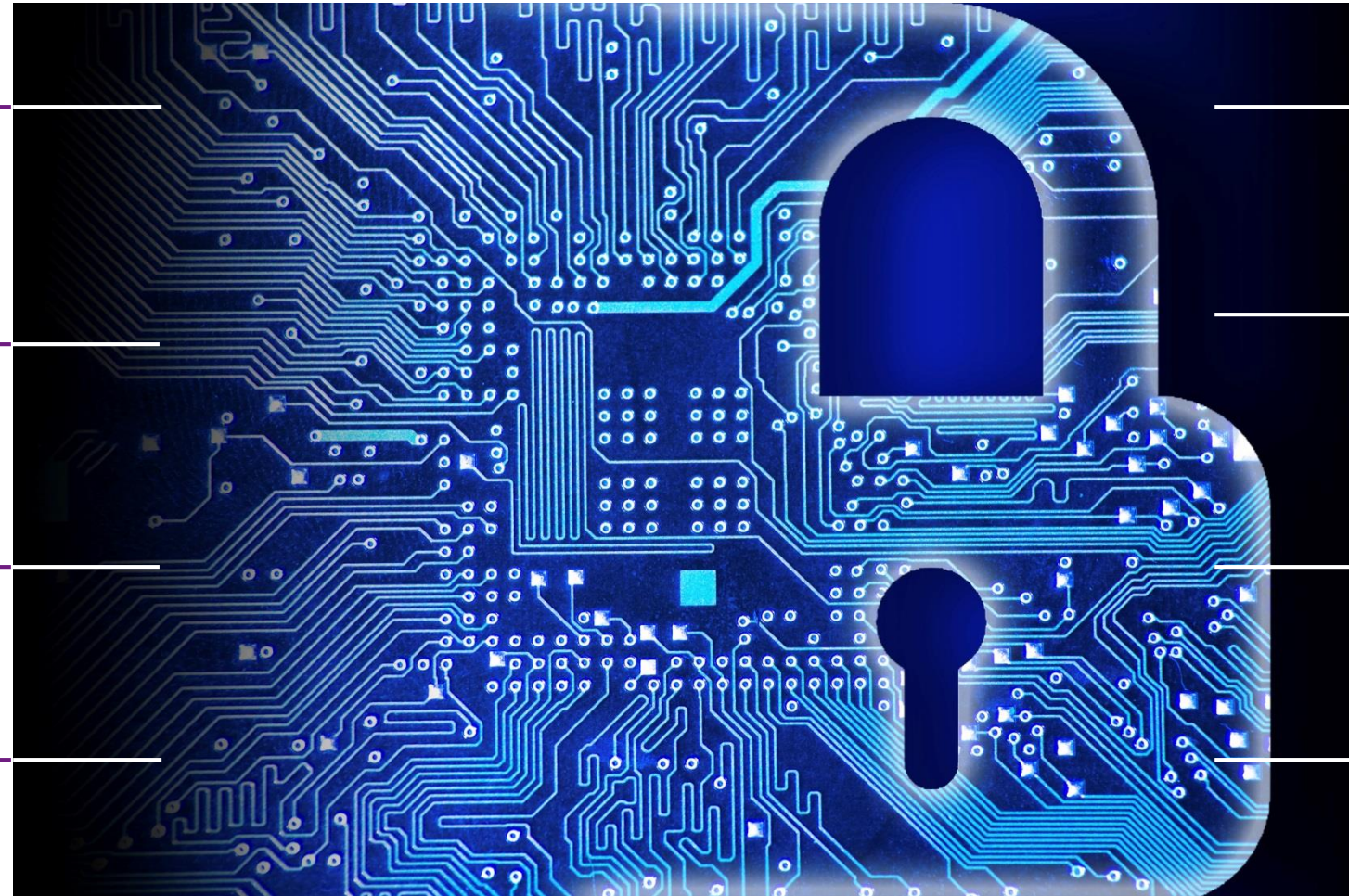
La Ciberseguridad es más compleja que nunca

Sobrecarga de Vendedores

Escasez de Talento

Presiones Regulatorias

Nuevos Ecosistemas Digitales



Incremento en Crimen Cibernético

Evolución de tecnologías en la nube

Más movilidad

Modelos disruptivos de negocio

El riesgo y las consecuencias

RIESGOS CLAVES	CONSECUENCIAS
<ul style="list-style-type: none">▪ Ataque de denegación de servicio▪ Ransomware▪ Actos negligentes de empleados, contratistas, proveedores▪ Ataques contra proveedores externos (riesgo de la cadena de suministro)▪ Recibo o transmisión de virus o malware▪ Acceso no autorizado por terceros▪ Uso no autorizado por parte de empleados, contratistas y proveedores de servicios	<ul style="list-style-type: none">▪ Daño a la Reputación– Pérdida de valor de marca y confianza del consumidor▪ Reclamos por terceros y reguladores▪ Interrupción de Negocio▪ Demandas de Extorsión▪ Pérdida de propiedad intelectual▪ Gastos de reparar o reinstalar sistemas▪ Costos de gestión de crisis▪ Daños Corporales▪ Daños a la propiedad

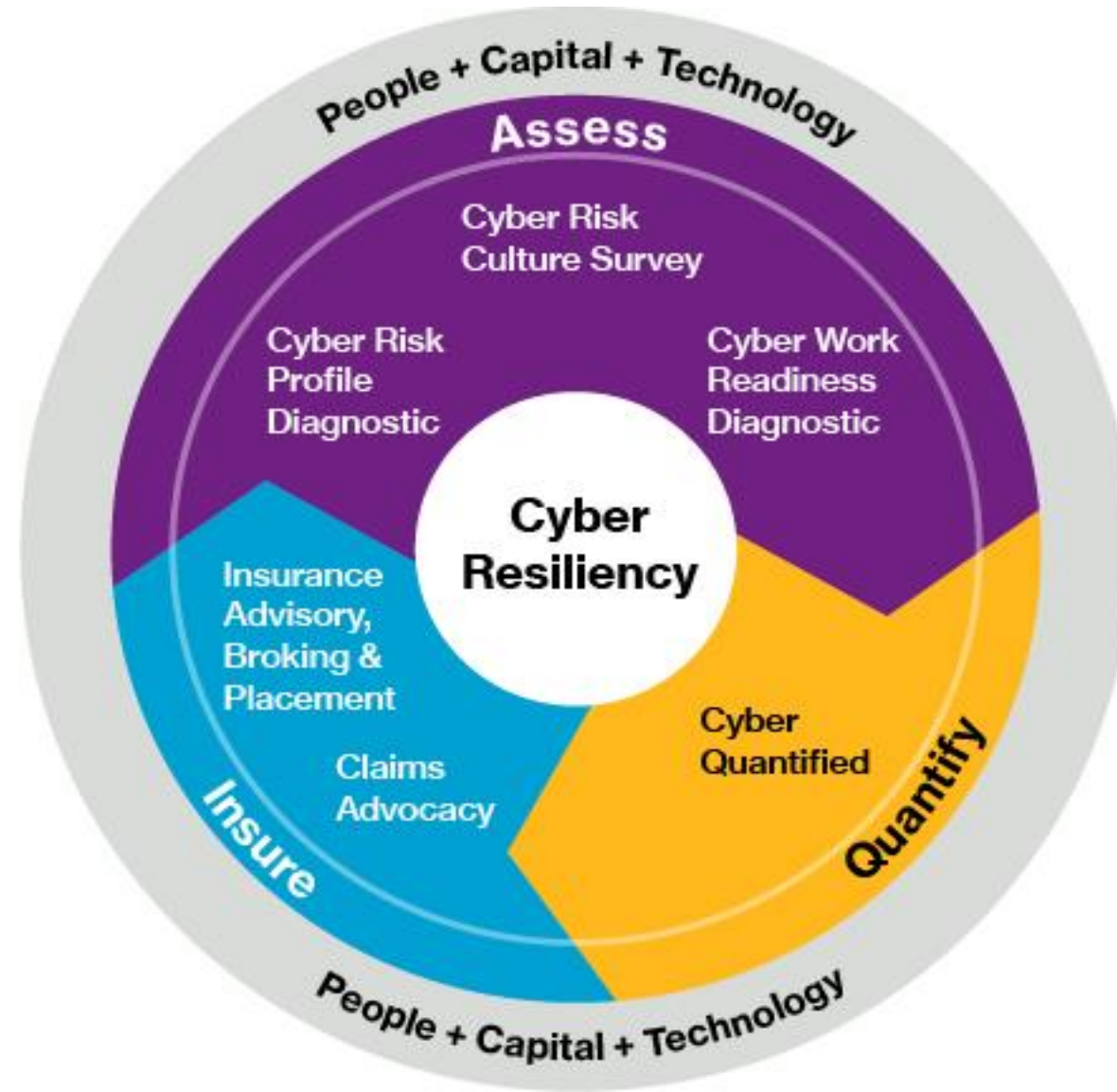
Ataques Cibernéticos



Evolución del Seguro Cibernético (1998 – 2018)



Soluciones Innovadoras para la Gestión de Riesgos Cibernéticos



Primer Paso: Evaluar el riesgo

Análisis y Entendimiento



Recopilación y análisis de la operación
Definición de la estrategia óptima a seguir para analizar y transferir el riesgo cibernético.



Cyber Risk Profile Diagnostic – CRPD, Diagnóstico del nivel de exposición a los riesgos cibernéticos en la Organización (por compañía/subsidiaria/geografía).



Análisis y cuantificación del peor escenario por riesgos cibernéticos con impactos diferentes a privacidad e interrupción de la red para la Organización.



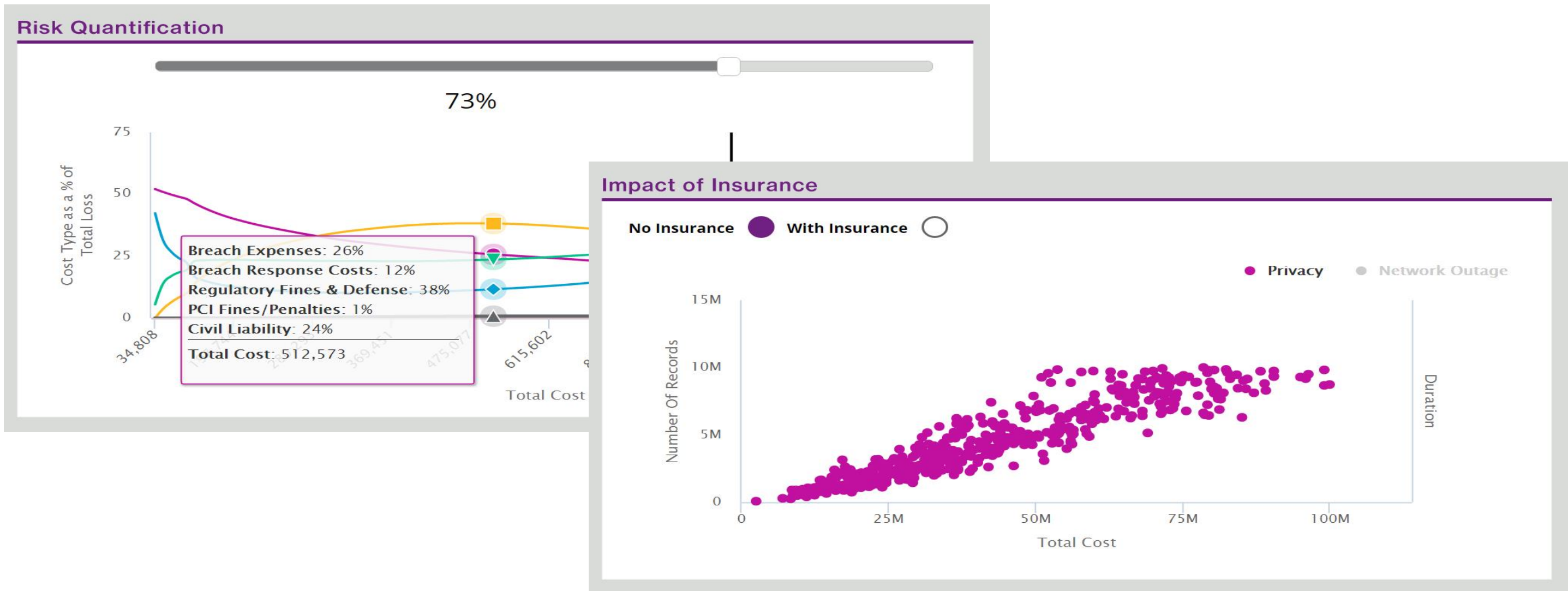
Encuesta de Cultura de Riesgo Cibernético, información sobre el riesgo de las personas para ayudar a los clientes a abordar las vulnerabilidades creadas por sus empleados



Cyber Work Readiness Diagnostic, un análisis de todas las funciones cibernéticas: ayuda a las organizaciones a desarrollar estrategias que definen la naturaleza y el alcance de su trabajo de ciberseguridad.

Segundo Paso: Cuantificar el riesgo

Cuantificación del nivel del riesgo cibernético – a través de nuestra herramienta **Cyber Quantified**; riesgo de violaciones a la privacidad o interrupciones a la red de la Organización o subsidiarias.



Tercer Paso: Asegurar/ Transferir el Riesgo



Pérdidas de Tercero por Privacidad y Seguridad de la Información

- Violación de información sensible de Tercero
- Corrupción o eliminación de Datos de Tercero
- Violación de información por parte de un proveedor externo
- Denegación de servicio o de códigos maliciosos a través de su propia red
- Robo o pérdida de Hardware o PC con información sensible conteniendo datos de Tercero
- Violación de la propiedad intelectual, plagio, difamación



Pérdidas Propias del Asegurado

Interrupción de la red debido a:

- Delitos informáticos
- Sabotaje de empleados
- Errores operativos y administrativos

Interrupción de Negocios

Restauración, reconstitución, recreación de activos digitales debido a:

- Delitos informáticos
- Sabotaje de empleados
- Errores operativos y administrativos

Cyber extorsión:

- Costos de contratación de expertos en gestión de crisis
- Costos de pago de rescates



Gastos Asociados

- Sanciones y multas inherentes a protección de datos
- Gastos de defensa e investigación de protección de datos
- Costos de Relaciones Públicas
- Gastos de notificación de violación de información
- Gastos de supervisión de robo de identidad / crédito

Que Sigue?

Incremento en demanda para productos que cubren pérdidas a consecuencia de un ataque cibernético que ocasione:



Daño material



Lesiones Personales



Responsabilidades Ambientales

Productos hecho a medida para diferentes Industrias dependiendo de sus necesidades

CyFly para Aerolíneas

- Interrupción debido a cancelaciones de vuelos causadas por interrupción en redes informáticas de terceros.
- Valor mínimo acordado opcional para cancelaciones de vuelos debido a la interrupción de la red
- Las multas y la indemnización de la aviación civil derivadas de una interrupción de la red.
- Cobertura para fraude de programa de viajero frecuente.

CyFi para Instituciones Financieras

- Pérdidas de tarjetas de plástico causadas por clonación o modificación de tarjetas tras un acceso no autorizado a un sistema de IF
- Pérdidas financieras causadas por:
 - Robo de datos confidenciales
 - Cyber terrorismo
 - Hackers aprovechando fallas técnicas y/o errores de diseño

2018 Cyber Risk Equipo del Año!

Premiada en la ciudad de Nueva York - Cena anual de premios
Cyber Risk Awards

