Que tan relevante es el Seguro de Cyber como un medio de gestión de riesgos para las infraestructuras criticas

Elizabeth Gurney
Cyber Product Champion, Latin America

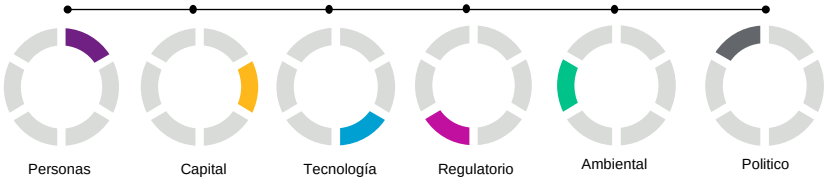
Willis Towers Watson

La sociedad está hiperconectada y el riesgo cibernético afecta todos los aspectos de la vida moderna.

Industrial Internet of Things (IIOT)

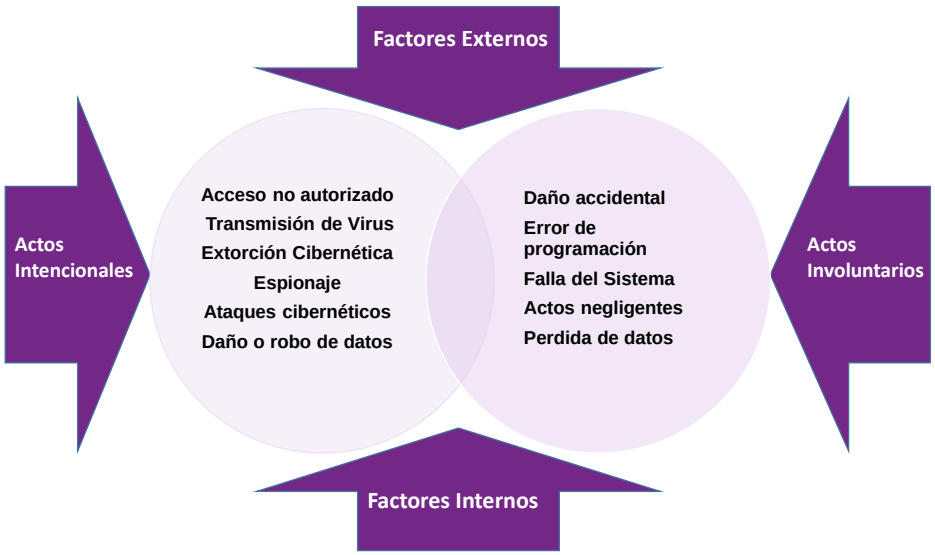
"Los ataques en contra de un sistema pueden involucrar solo los componentes cibernéticos y su operación, pero esos impactos pueden extenderse a los sistemas físicos, comerciales, humanos y ambientales a los que están conectados."

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



SEMINARIO
Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades

Los Riesgos Cibernéticos



Industria	Riesgo vinculado a Cyber (dentro de los primeros 10 del WTW Industry Index)
Tecnología, medios y telecomunicaciones	#4 Ataques y secuestros cibernéticos
Financiera	#4 La digitalización creando nuevos riesgos como ciberataques
Transporte	#1 Mayores amenazas en términos de seguridad provenientes de violaciones cibernéticas y la privacidad de datos
Recursos Naturales (O&G, Minería, Generación Eléctrica)	#3 Incremento en ciber-seguridad y riesgos de privacidad de datos
Construcción	#9 Incremento de seguridad relacionado a ciberataques y violaciones de la privacidad de datos

SEMINARIO
Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades

Vulnerabilidades en Tecnología Operativa (OT)

- Software antiguo y sistemas heredados
- Inactividad para mantenimiento y parches a menudo no es posible
- Conectividad con el Internet
- Conectividad con la red de TI

Ciberataques a Infraestructura Critica

Virus “Stuxnet” afecto a varias centrales nucleares en irán. Fue planteado por una persona atreves de una memoria USB. El objetivo era los “Programable Logic Controllers” y a través de esos “controllers” lograron controlar la velocidad de los centrifugadoras utilizados para producir uranio. Al cambiar el tiempo del giro podían destruir el uranio.

Perdida:

Causo un daño sustancial al programa nuclear de Irán al destruir su uranio.

Afecto a tres empresas de energía eléctrica en Ucrania. El Malware obtuvo acceso a los redes corporativos y luego salto al sistema SCADA. Utilizaron instrucciones legitimas para desconectar subestaciones de la red. Malware también borro todo de las sistemas Windows y destruyo los “Serial to Ethernet” aparatos.

Perdida:

Por un periodo de 6 horas, 225,000 personas estaban sin energía. Tenían que operar sin SCADA y control automatizados por más de un año en algunas sitios

INDUSTROYER

SEMINARIO
Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades

Los ciberdelincuentes tomaron control del software de producción en una planta de acero alemana y causaron importantes daños materiales en el sitio. Los atacantes primero piratearon la red informática y a partir de esta red, penetraron en el software de gestión de producción de la planta. Accedieron a la mayoría de los sistemas de control de la planta y destruyeron metódicamente los componentes de interacción humana. Lograron evitar que un alto horno iniciara su configuración de seguridad a tiempo y causó daños graves a la infraestructura.

Perdida:

Causó daño severo al alto horno

En el caso del malware Triton, se dirigió directamente a las redes de OT. Los atacantes, supuestamente como un estado-nación (que luego se pensó que sería Irán), lograron obtener acceso remoto a una estación de trabajo de ingeniería en Arabia Saudita. El ataque aprovecho de fallas en los procedimientos de seguridad y, en última instancia, una vulnerabilidad desconocida en el firmware del sistema de seguridad Triconex Tricon de Schneider.

Perdida:

Tenía la intención de sabotear las operaciones de la empresa y desencadenar una explosión, sin embargo, una falla en el código de los atacantes cerró accidentalmente el sistema.

MERCK Research Laboratories

En Julio del 2017, la empresa farmacéutica fue afectada por el virus Not Petya - eso llevó a una interrupción de sus operaciones en todo el mundo, incluidas las operaciones de fabricación, investigación y ventas.

Perdida:

USD 620 millones o más en el 2017 y se esperan más pérdidas en 2018.

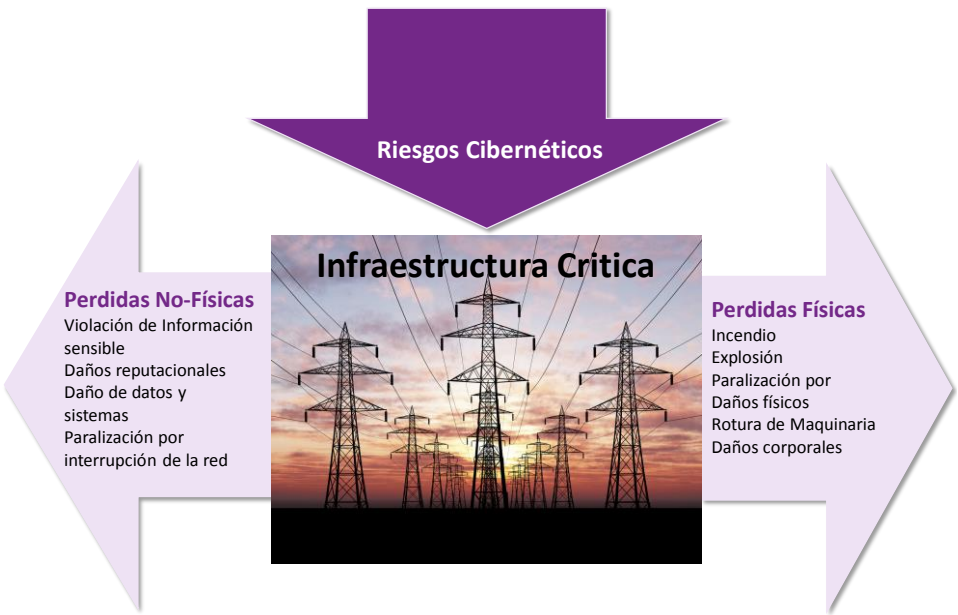
En Julio de 2017 la compañía de envió de contenedores más grande del mundo fue afectada por el virus Not Petya – eso afecto a sus operaciones y comunicaciones de una forma significativa.

Perdida:

Tenían que reinstalar más de 4,000 servidores, 45,000 computadoras y 2,500 aplicaciones en el transcurso de 10 días en el julio del 2017. Costo mas de USD 300 millones de dolares.

MAERSK

SEMINARIO
Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades



Metodología para la transferencia del riesgo cibernético

Etapa 1
Análisis y Entendimiento

- •Recopilación y análisis de la operación del cliente.
  •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
- Cuantificación del nivel del riesgo cibernético – a través de nuestra herramienta **Cyber Quantified** que impliquen violaciones a la privacidad o interrupciones a la red.
- Análisis y Evaluación de los riesgos cibernéticos del cliente - Taller de Evaluación **Cyber RAPID**.
- Análisis y cuantificación del peor escenario por riesgos cibernéticos con impactos diferentes a privacidad e interrupción de la red.

Etapa 2
Construcción de la póliza

- Análisis de Coberturas por medio de la revisión de las pólizas actuales con la finalidad de identificar los vacíos que se puedan presentar.
- Identificación de las necesidades de cobertura y definición de los amparos, con base en los resultados de la etapa 1 y del análisis de coberturas:
  - Estructura clausulado a la medida y slip de condiciones.

Etapa 3
Estrategia de Colocación de la póliza

- Estrategia de aproximación al mercado y definición de los aseguradores y reaseguradores adecuados para el riesgo.
- Proceso de colocación y Transferencia del riesgo.

SEMINARIO
Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades

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.
- **Diagnostico** 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.
- **Analizar** información sobre el riesgo de las personas para luego abordar las vulnerabilidades creadas por sus empleados
- Análisis de todas las funciones cibernéticas dentro de la empresa para luego desarrollar estrategias que definen la naturaleza y el alcance de su trabajo de ciberseguridad.

Segundo Paso: Análisis de Coberturas – Identificación de Vacíos

Identificación de Necesidades
Asesoría y análisis de los riesgos cubiertos, y no cubiertos. Actualización respecto a nuevas coberturas

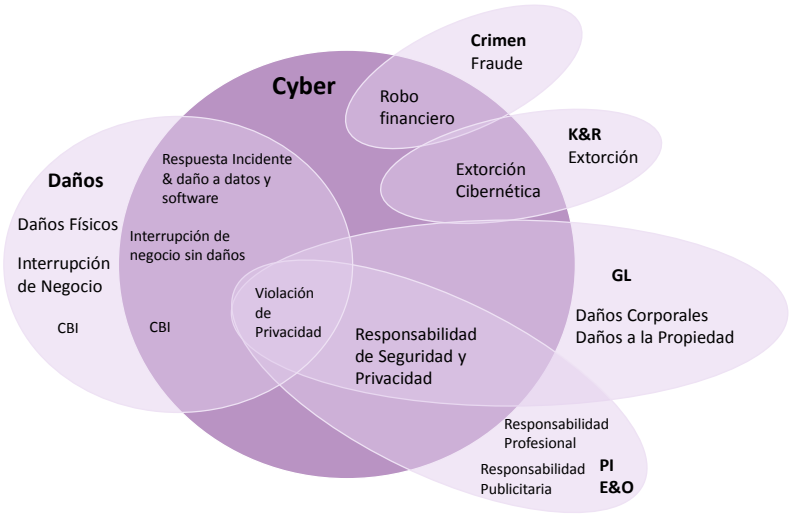
Análisis de Coberturas en las pólizas de IRF, RCE, D&O, PI, Daños Materiales:

- Análisis de las coberturas de riesgos cibernéticos que se puedan encontrar en las otras pólizas de programa, con el fin de alinear las coberturas
- Identificación de vacíos de riesgos cibernéticos en las demás pólizas del programa.
- **Finalidad:** Lograr unificación en el programa de seguros respecto de los riesgos cibernéticos de la empresa.

Rioesgos Cibernéticos	Seguros					
	Crimen / Bankers Blanket	Responsabilidad General	Directores & Administradores	Responsabilidad Profesional	Propiedad / Lucro Cesante	Cibernético
I. PÉRDIDAS DE TERCEROS POR PRIVACIDAD Y SEGURIDAD DE DATOS						
Violación a la Información Sensible de Terceros						
Violación de Datos causada por un Proveedor Externo						
Corrupción de datos de Terceros por un Código Malicioso						
Denegación de Servicio Distribuido o Código Malicioso enviado vía su propia red						
Corrupción o Eliminación de Datos de Terceros						
Perdida/Robo de portátiles o Hardware que contenga información sensible						
Violación de datos debido a Violacion de la Seguridad.						
Violación de Propiedad Intelectual, Plagio y Difamación						
II. PÉRDIDAS PROPIAS POR VIOLACIÓN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN						
Protección de Datos: Multas y Sanciones						
Protección de Datos: Gastos de Defensa e Investigación						
Costes de Relaciones Publicas						
Protección de Datos: Gastos Legales						
Gastos de Notificación por Violación de Datos						
Gastos de Monitoreo de Robo de Identidad /Crédito						
III. PÉRDIDAS PROPIAS: RIESGOS CIBERNÉTICOS						
Interrupción de la red por:						
• Delitos Informáticos						
• Sabotaje de Empleados						
• Errores Operativos y Fallos Administrativos						
Restauración, Recogida, Recreación de Activos digitales por:						
• Delitos Informáticos						
• Sabotaje de Empleados						
• Errores Operativos y Fallos Administrativos						
• Daño Accidental al Hardware						
Extorsión Cibernética						
IV. PÉRDIDAS PROPIAS DAÑOS MATERIALES						
Lucro Cesante derivado de daños materiales						
Lesiones personales como consecuencia de un daño material						

SEMINARIO
Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades

Cobertura "silent" para riesgos cibernéticos dentro de otras pólizas de seguros



Fuente: SCOR

Tercer paso transferir su riesgo al mercado de seguro

$3.0b (2017)

Estimado Prima Bruto Global del Seguro Cyber

Capacidad disponible para un solo riesgo:

$600m para un solo cliente

***cobertura** = protección

80% de las empresas **Fortune 1000** compran un seguro cibernético

$17b

Tamaño estimado del **Mercado del Seguro Cibernético** en 2023

$6t

Costo estimado de Cibercrimen a la economía global en 2021

Proveedores claves del Seguro
***(Mercados/suscriptores)**

AIG
XL Catlin
Beazley
Chubb
Lloyd's

En 2017, El reclamo promedio para una empresa grande era $3.2M

$6b

Daños globales estimados de***ransomware** para 2017

60+

aseguradoras que ofrecen el seguro Cyber

***ransomware:** un tipo de software que restringe los datos y exige al usuario pagar un rescate para eliminar la restricción

SEMINARIO
Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades

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 no esta cubierto por la póliza de cyber?

- Pérdida de, o daño a, cualquier propiedad física. Aunque existen algunas **coberturas especiales**.
- Cualquier falla o interrupción de servicios externos de energía, servicios públicos, satélites o telecomunicaciones
- Actos intencionales o fraude del equipo directivo
- Brechas o fallas que comenzaron antes de la fecha de retroactividad
- Actualizaciones o mejoras del sistema
- Crimen financiero – el robo de dinero o valores. Aunque se puede conseguir sublimites de cobertura.

SEMINARIO
Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades

Coberturas especificas

Daño a propiedad | **Lesiones Personales** | **Responsabilidades Ambientales**

- **Exclusiones especificas** en las pólizas tradicionales:
- CL380
- Exclusión NMA 2914
- Texto LMA 3030, exclusión 9

Cobertura bajo 2 modalidades:

- Como parte de las coberturas de Incendio o de Responsabilidad Civil General de la Empresa en forma de un “write back”
- Cobertura como parte de la póliza de Cyber

Características:

- Mercado limitado
- Costo de seguro similar al costo de una póliza de daños/incendio

Ejemplo de las coberturas en acción

Se Descubre un incidente	Evaluación del incidente	Manejo de Crisis a Corto Plazo	Manejo de Consecuencias
▪ Ocurre el evento	▪ Investigaciones forenses y apoyo legal	▪ Notificación a terceros y Monitoreo de crédito ▪ Relaciones Públicas ▪ Manejo de ciberextorción (incluyendo el pago del rescate) ▪ Restauración de datos y sistemas (informáticos y operacionales)	▪ Acciones legales de terceros ▪ Interrupción de negocio ▪ Perdidas físicas como consecuencia de un ciberataque

Muchas Gracias por su atención!

Elizabeth Gurney
Cyber Product Champion, Latin America

Willis Towers Watson