El cibermercado en evolución

Conferencia ICMIF/Américas 2017

CYBERSCOUT®

1

¿Quién es CyberScout?

Educa. Protege. Resuelve.

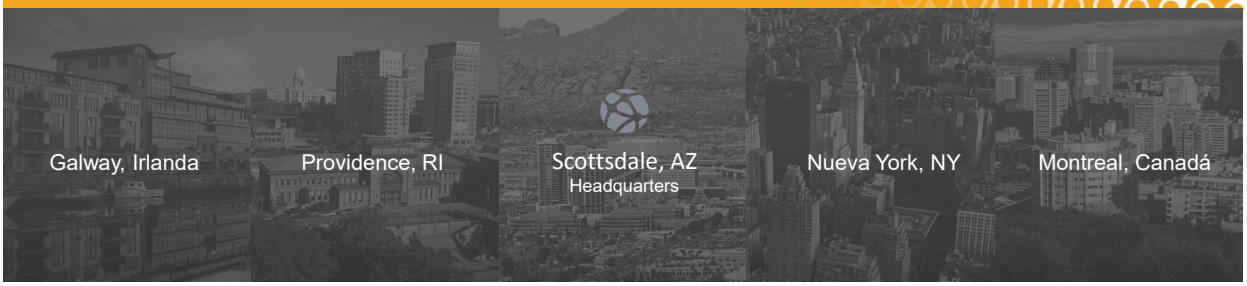
Por más de 14 años, CyberScout ha sido una referencia líder en servicios de defensa de datos e identidad. Nuestra reputación de larga data, experiencia en la industria y enfoque escalable ofrecen a las empresas y sus clientes un aliado de confianza para:

- Gestión de identidad
- Educación, preparación, respuesta y remediación de filtración de datos
- Monitoreo de reputación, fraude y crédito
- Consultoría de Privacidad de datos y Ciberseguridad

CYBERSCOUT

3

Alcance mundial actual



660+
Instituciones

17.5
Millones de hogares

45
Millones de individuos

770 000
Clientes Servicios Filtración

CYBERSCOUT

2

Comprender los riesgos

Filtración de datos - Titulares

Three Mobile cyber hack: six million customers' private information at risk after employee login used to access database

500 million Yahoo accounts breached

Security

Sports Direct hacked last year, and still hasn't told its staff of data breach

UK firms could face £122bn in data breach fines in 2018

Hackers publish contact info of 20,000 FBI employees

Energy facility cyber incidents rose nearly a third last year, DHS says

UCF data breach: 63K Social Security numbers compromised

Monday 13 March 2017 1:36pm

Three Mobile cyber attack: Mounting numbers of customers hit following November breach

Cyber-Safe

Cyber thieves siphon tax forms from ADP payroll data

NEWS

Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords

The Switch

The human problem at the heart of Snapchat's employee data breach

CYBERSCOUT

¿Cómo sucede la exposición de la información?

Error del personal

"Empleado de la Universidad publica por error en la red información personal de estudiantes inluidos sus NSS (número seguro social)"
- SC Magazine

Desecho de documentos

"La organización Samaritan Health Services investiga luego de encontrar registros médicos en la basura"
- Gazette-Times

Desecho de disco duro

"Compañía multada por dejar datos electrónicos de salud en el disco duro de fotocopiadora alquilada"
- CNS News.com

Acceso no autorizado

"Empleado de salud de Florida despedido al ser descubierto fotografiando datos de paciente"
- SC Magazine

CYBERSCOUT

¿Cómo sucede la exposición de la información?

Piratería informática

"Robo de información de 1,4 millones de usuarios, incluidos datos de tarjeta de pago"
- IB Times, UK Edition

Pérdida o robo

"Laptops con datos de pacientes robados de clínica médica"
- WSPA.com

Error de correo

"Centro médico envía por correo 63.000 cartas con información personal a destinatarios incorrectos"
- SC Magazine

Distribuidores

"Proveedor de Programa Hospitalario sufre filtración de datos de información personal de los empleados"
- SC Magazine

CYBERSCOUT

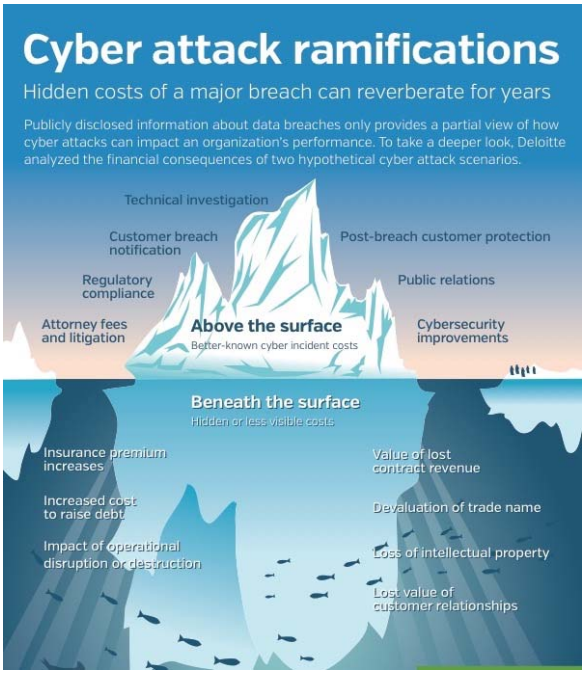
Aprovechamiento y ciberataques comunes

- Ingeniería social
- Ransomware
- Ataques DDoS/DoS
- Zero Day Vulnerability
- Código malicioso/Malware
- Spyware
  - Key logger
- Spoofing
- Los “Ishes”
  - Phishing, Spear-phishing, Vishing, SMiShing and Whaling

CYBERSCOUT

En 82% de los casos, la organización se ve comprometida en cuestión de minutos

- “Data Breach Investigations Report,” Verizon



Un estudio de Deloitte de 2016 descompone los costos conocidos y no tan conocidos de un ciberataque. Los costos “por debajo de la superficie” pueden ser de largo plazo y devastadores.

Los ejemplos incluyen:

- Pérdida de relaciones con clientes
- Impacto reputacional
- Protección de clientes
- Notificaciones
- Interrupción del negocio

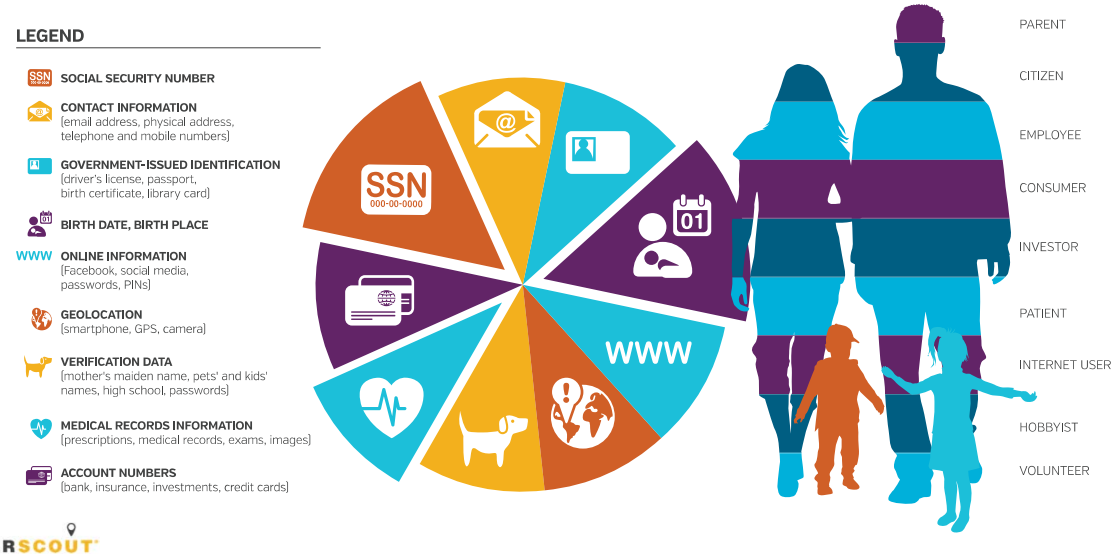
¿A quién apuntan los ciberdelincuentes?

- **Grandes compañías** que colectan, almacenan o transmiten datos sensibles
  - Empresas aseguradoras, instituciones financieras, proveedores de beneficios para empleados, gobiernos, hospitales, etc.
- **Empresas pequeñas y medianas (EPM)** desde locales tradicionales a servicios en línea.
  - 28 millones de propietarios de pequeñas empresas no confían en su seguridad[1]
  - 43% de los ciberataques a nivel mundial van dirigidos a empresas con menos de 250 trabajadores[2]
  - 1 cada 5 EPM denunciaron un ciberataque[3]
  - 48% denunciaron que los ciberataques produjeron interrupción del servicio[4]
  - El costo promedio de una filtración para una empresa pequeña o mediana superó los $180K[4]
- **Cliente final (Individuo)**
  - Desde errores humanos –una billetera perdida – a riesgos emergentes como el internet de las cosas, dispositivos móviles, hogares conectados y ataques DDoS

CYBERSCOUT

En pocas palabras, ¡TODOS somos potenciales objetivos!

¿Qué información está en riesgo?



CYBERSCOUT

Las empresas que manejan IPI están en peligro

Registro de empleados

- Información de contacto
- ID emitido por el gobierno
- Fecha y lugar de nacimiento
- Números de cuentas

Información de pago

- Información online
- Información de contacto
- Números de cuentas

Tarjetas fidelidad

- Información online
- Información de contacto
- Fecha y lugar de nacimiento
- Números de cuentas
- Datos de verificación

Proveedores 3ras Partes

- Información de contacto
- ID emitido gobierno
- Fecha y lugar de nacimient
- Números de cuentas
- Online Info Información
- Datos de verificación
- Info registros médicos

CYBERSCOUT

Ejemplo de empresas en riesgo

Construcción

- Datos empleo
- Test drogas
- Registros médicos
- Info pagos
- Propiedad intelectual

Inmobiliaria

- Datos empleo
- Número seguridad social
- Gov't-issued IDs
- Informés crédito

Transporte

- Datos empleo
- Tracking GPS
- Info pagos

CYBERSCOUT

Definición del problema

- **Las filtraciones pueden ser aterradoras** tanto para los individuos como para las empresas.
  - *Las víctimas necesitan acceso a educación preventiva de valor, a servicios de protección proactivos, y soluciones rápidas y apropiadas a los incidentes.*
- **Las víctimas necesitan un socio confiable** que haga lo imposible para lograr una resolución satisfactoria.
  - *Las aseguradoras, las instituciones financieras y los empleadores son el primer lugar al que recurren las víctimas en busca de ayuda/consejo.*
- **La pérdida de negocios es la principal consecuencia financiera** que experimentan las organizaciones que sufren filtración de datos.
  - *Luego de la filtración de datos, las organizaciones necesitan de un socio que las ayude a tomar los pasos para retener la confianza de los clientes y así reducir el impacto financiero a largo plazo.*

CYBERSCOUT

15

Definición del problema

- **Las regulaciones de ciberseguridad están en evolución** y las organizaciones necesitan consejo de expertos para seguir siendo competitivos y cumplir con las normas.
  - *A medida que los reguladores cambian su enfoque pasando de la asistencia posfiltración a los requerimientos prefiltración para mitigar los riesgos, las organizaciones de todos los tamaños necesitan expertos que las preparen para los cambios.*
- Las organizaciones que realizan mejoras a sus **programas de gobernanza de datos pueden reducir el costo de una filtración de datos**.
  - *El desarrollo de planes de respuesta a incidentes, la designación de un CISO, programas de capacitación y concientización para empleados, y una estrategia de continuidad, todo esto resulta en una reducción de costos.*

CYBERSCOUT

16

3

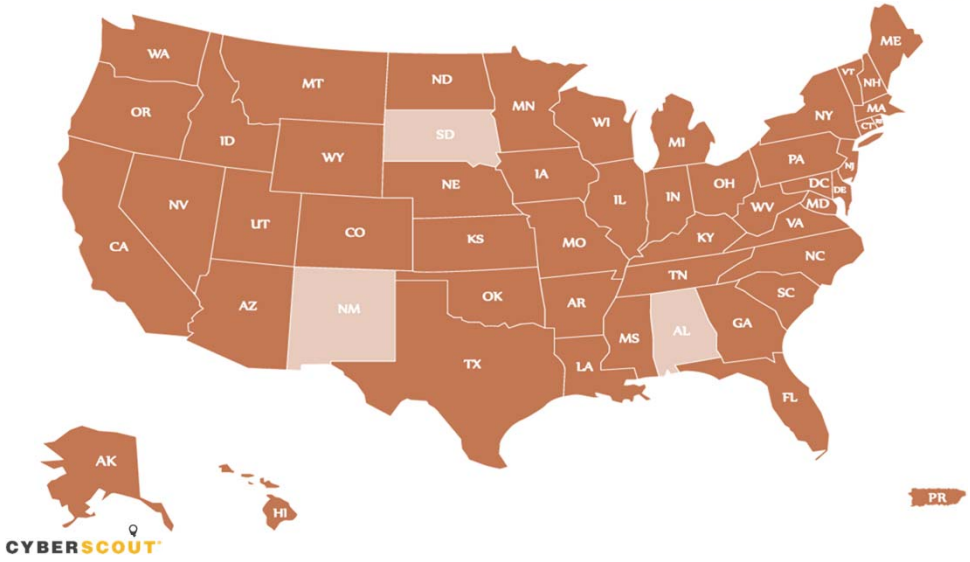
Evolución de la privacidad y regulación de la filtración de información

Enfoque regulatorio originado por la OCDE

8 principios centrales para que los controladores de datos cumplan bajo cualquier regulación:

CYBERSCOUT

Cyber U.S. comienza con Leyes de Notificación de filtración



48 estados, el Distrito de Columbia, Guam, Puerto Rico e Islas Vírgenes requieren la notificación de violaciones de seguridad que involucre PII

CYBERSCOUT

La próxima ola de regulaciones cibernéticas

- Ley de Privacidad Digital de **Canadá** que modifica la Ley de Protección a la Información y Documentos Electrónicos (PIPEDA) que agrega los requerimientos de notificación de filtración de datos y denuncia
- El Departamento de Servicios Financieros de **Nueva York** (NYDFS) dispone que las entidades a las que regula deben implementar estrictos requerimientos de ciberseguridad
- La Reglamentación General de Protección de Datos de la **Unión Europea** (GDPR) que refuerza la protección de datos para individuos en la UE, que agrega los requerimientos para la noticación y denuncia de filtración de datoss
- El programa Privacy Shield entre UE y EE.UU. que reemplaza al Safe Harbor para así brindar una mayor protección de los datos personales y facilitar el comercio digital a cada lado del Atlántico
- La ley enmendada de **Japón** sobre la Protección de Información Personal (diciembre 2016, entra en vigencia completa el 30 de mayo de 2017)
- Los comunicados de la DPA de **Argentina** que proponen un proyecto para actualizar las reglamentaciones existentes que transforma a la DPA en un regulador independiente con más poder.

CYBERSCOUT

Regimenes latinoamericanos actuales sobre la filtración de datos

CYBERSCOUT

1

Requisitos latinoamericanos de filtración de datos

Notificación de filtración de información en América Latina

Países con notificación de filtración (Aviso obligatorio)

Key: Texts in force | ✓ Texts in force | ⚠ Bill Pending | ✗ No requirement

Country	Mandatory notification required	Notification to consumer	Notification to regulatory authorities	Notification to other agencies
Latin America				
Chile	✓	✓	✓	✗
Colombia	✓	⚠	✓	✗
Costa Rica	✓	✓	✓	✗
Ecuador	✓	✓	✓	✓
Mexico	✓	✓	✗	✗
Uruguay	✓	✓	✗	✗

CYBERSCOUT

23

2

Filtración de datos en América Latina por país.

Chile

- **Primer país latinoamericano en aprobar leyes de protección de datos**
- Ley No. 19.628 sobre *Proteccion de la Vida Privada* (1999)
  - Ausencia de cualquier disposición relacionada a los requisitos de notificación sobre la filtración de datos.
- La notificación sobre la filtración de datos de la Ley del Chilena del Consumidor apenas se implementa.
- Ley No. 19.496 (1997)
  - El artículo 46 exige que un proveedor de servicios notifique a sus clientes en casos de contingencia o riesgos asociados con su producto o servicio.
  - El artículo 3 otorga derechos del consumidor a la seguridad de servicios/productos y prevé resarcimiento a través de la indemnización por daños
  - NO hay disposición que requiera la notificación por filtración de datos personales
    - La obligación es inferida, no hay condiciones específicas para la notificación

CYBERSCOUT

25

Costa Rica

- **Ley sobre la Protección Individual para el Procesamiento de Datos Personales ('la Ley') y el Decreto Ejecutivo N° 37554**
- El artículo 38 del Decreto regula las filtraciones generles de datos
  - *"Cualqueir irregularidad en el tratamiento o almacenamiento de los datos, como ser la pérdida, destrucción o cualquier otra filtración de datos"*
- El artículo 39 indica que el controlador de datos (la parte responsable de los datos) debe informar a interesado y a la Autoridad de Protección de Datos de cualquier tipo de vulnerabilidad que pueda surgir.
  - Dentro de los cinco (5) días hábiles
    - ✓ Notificación exigida a los interesados y la DPA
    - ✓ Debe iniciarse una revisión integral para determinar la extensión del problema y cualquier tipo de acción correctiva o preventiva

CYBERSCOUT

26

Ecuador

- **NO hay un requerimiento claro de filtración; se cubre bajo distintas regulaciones que se solapan, incluido:**
- La Constitución de la República de Ecuador
  - Garantiza protección de los datos personales incluido el acceso y las restricciones al cobro, almacenamiento, procesamiento, distribución y circulación.
- Ley Órgánica del Sistema Nacional del Registro de Datos Públicos
  - Define a los datos personales como: ideología, afiliación política, etnicidad, estado de salud, orientación sexual, religión, información financiera y de crédito, y cualquier otro tipo de datos relacionados a la privacidad e intimidad de la persona
- Ley Orgánica de Datos Civiles y Gestión de Idetidad
  - Crea un registro de datos personales ('Registro Personal Único' [RPU])
- Comercio electrónico, Mensajes de datos y Ley de firma electrónica

CYBERSCOUT

27

México

- La *Ley Federal y las Reglamentaciones sobre la protección de datos personales por partes privadas*requiere la notificación de filtración de datos a los interesados bajos circunstancias específicas
- Las violaciones de seguridad que se produzcan *en cualquier etapa* del procesamiento, que afecten de manera significativa la propiedad o los derechos morales de un interesado deberán informarse inmediatamente, para que puedan tomarse las acciones apropiadas para proteger sus derechos.
  - Las violaciones de seguridad que pueden ocurrir *en cualquier etapa* del procesamiento son:
    - ✓ pérdida o destrucción no autorizada;
    - ✓ robo, extravío o copia no autorizada;
    - ✓ uso, acceso o procesamiento no autorizado; o
    - ✓ daño, alteración o modificación no autorizada

CYBERSCOUT

28

México

- Las reglamentaciones establecen que el controlador de datos debe notificar al interesado de por lo menos lo siguiente:
  - ✓ Naturaleza de la violación;
  - ✓ Datos personales comprometidos;
  - ✓ Recomendaciones a los interesados sobre las medidas que pueden adoptar para protegerse;
  - ✓ Acciones correctivas implementadas; y
  - ✓ Cómo los interesados pueden obtener más información sobre la violación.
- Actualmente:

➢ no se requiere notificación de la DPA, solo notificación a los interesados

➢ La DPA no he emitido ninguna aclaración sobre qué se considera un daño *"significativo" a la propiedad o derechos moreales de un interesado*.

CYBERSCOUT

29

Uruguay

- La notificación de violación se aplica de manera laxa con al excepción de requerimientos específicos para telecoms.
- Similar a los requerimientos de notificación de violación en la UE.
- La *Ley 18.331 sobre la Protección de Datos Personales y la Acción de Habeas Data y el Decreto 414/009* regula los requerimientos de protección de los datos personales.

➢ El artículo 10 reglamenta específicamente las medidas de seguridad para proteger datos personales y asegurar su integridad, confidencialidad y disponibilidad. El Decreto también establece el requerimiento de notificación para las filtraciones de datos generales.

➢ El artículo 20 refiere a la protección de datos personales *específicamente* en el sector de las telecoms.

CYBERSCOUT

30

4

¿Qué es la cobertura cibernética?

Tendencias de seguro cibernético

- El ciberseguro es una enorme oportunidad, todavía bastante inexplorada, para aseguradoras y reasguradoras.
- Cualquier organización que almacene y mantenga información del cliente (PII), recoja información de pagos en línea, o utilice la nube considera el ciberseguro.
- PwC estima que las primas brutas emitidas crecerán de aproximadamente de $2.500 millones hoy a $5000 millones en 2018 y podrían llegar a los $7.500 millones o más para 2020
- 90% de los ciberseguros lo compra las empresas de EE.UU. pero solo una tercera parte de las empresas en EE.UU tienen algún tipo de cibercobertura.
  - Existe una amplia variación en la aceptación por parte de la industria, con solo el 5% de las compañías manufactureras en los Estados Unidos que poseen un seguro cibernético independiente, en comparación con alrededor del 50% en los sectores de salud, tecnología y venta minorista.
- En el Reino Unido, solo alrededor del 2% de las empresas cuentan con un seguro cibernético independiente

CYBERSCOUT

Fuente: PwC Insurance 2020 & beyond: Reaping the dividends of cyber resilience

Mercados de seguros cibernéticos

THE NUMBERS

32+	30+	9+
Domestic Markets	Lloyd's syndicates	Bermuda Markets

16	Number of years that a dedicated policy has been offered
$3B	Total estimate of current annual premium placed in the market
$500M	Largest cyber stand-alone program placed in the market
27%	Increase in purchasers in 2016, following 32% and 21% in years prior

CYBERSCOUT

Resumen de seguro cibernético

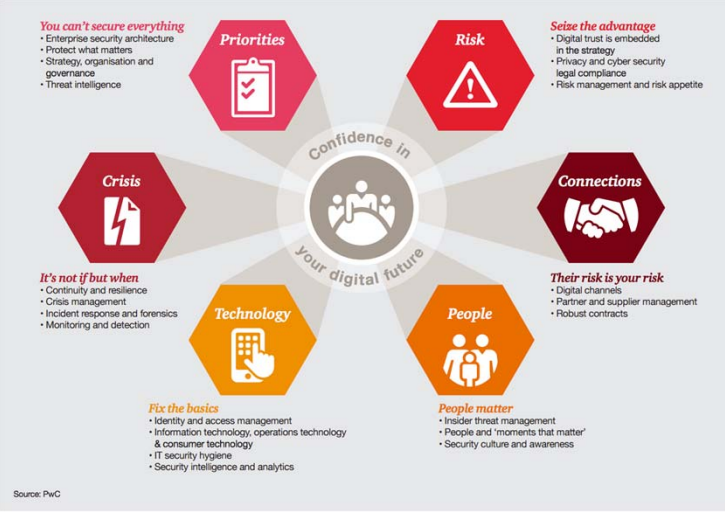
- Una política de seguro cibernético (riesgo/responsabilidad) está diseñada para ayudar a una organización a mitigar la exposición al riesgo compensando los costos relacionados con la recuperación después de una violación de seguridad relacionada con el ciberespacio o un evento similar.
- Se expandieron los orígenes de los errores y omisiones (E & O) de las compañías tecnológicas para abordar
  - producto de software que colapsa la red de otra empresa
  - acceso no autorizado al sistema de un cliente
  - destrucción de datos
  - virus con impacto sobre un cliente
- Actualmente, el seguro cibernético cubre los gastos relacionados con las primeras partes, así como los reclamos de terceros.
  - Aborda investigaciones forenses, pérdidas comerciales, costos de notificación de violación de datos y representación legal.

CYBERSCOUT

Tendencias de seguro cibernético

- La capacidda del ciberseguro **continuará aumentando**
- **Crea presión a la baja en las tasas de primas**
- Algunas aseguradoras pueden competir relajando límites, exclusiones y otros términos y condiciones
- Es importante comprender las motivaciones y los factores que explican por qué las empresas están comprando cibercobertura junto con sus riesgos potenciales

CYBERSCOUT



Explicación de Acuerdos de Seguro

Cobertura terceros	**Errores & Omisiones (E&O)**	La cobertura de los costos de defensa y los daños que surjan de las denuncias de actos, errores, omisiones o negligencia en la prestación de servicios a los demás Puede incluir Tech especializado E & O o cobertura de responsabilidad profesional miscelánea.
	Seguridad/Privacidad	Cobertura de costos de defensa y daños que surjan de 1) falla o violación de la seguridad de un sistema informático o red o 2) falta de protección de información confidencial o cualquier violación de un estatuto de privacidad federal, estatal, extranjera o local. Puede incluir cobertura para multas PCI, sanciones y/o evaluaciones.
	Regulatorio	Cobertura de los costos para responder a una investigación gubernamental que surja de un evento de privacidad. Incluye cobertura para multas y sanciones en la medida permitida por la ley.
	Medios	Cobertura de reclamos de terceros que aleguen difamación, calumnia, infracción de derechos de autor / marca registrada, invasión de privacidad, etc. que surjan de todo el contenido distribuido por una empresa.
Cobertura de primera parte	**Respuesta a la violación**	Cobertura de los costos para responder a una filtración de datos, incluidos los costos para realizar una investigación (incluidos los costos forenses) en cuanto a la causa del evento, costos de relaciones públicas, costos de notificación, costos para ofrecer servicios de control de crédito / robo de identidad.
	Interrupción de redes	La cobertura por pérdidas del asegurado luego de una falla de seguridad (por lo general luego de un período de espera y sujeto a una retención monetaria) Los costos asegurables pueden incluir gastos extra originados por la interrupción e ingresos perdidos.
	Restauración de datos	Los costos de restaurar/recrear los datos electrónicos luego de un fallo o violación de seguridad de un sistema informático.
	Ciberextorsión	Cobertura por la pérdida incurrida por el asegurado por el dinero pagado con el consentimiento de la aseguradora para resolver una amenaza de seguridad cibernética y los costos para investigar la causa de la amenaza.

36

Explicación de coberturas auxiliares

Cobertura

Abogados empleados (CCP)	Cobertura de pasivo por costos de defensa y daños que surja del trabajo realizado por abogados empleados. Incluye cobertura de las acciones de los abogados al tiempo que proporciona servicios gratuitos y pluriempleo.
Guarda a la reputación	Cobertura de primera parte para los costos de relaciones públicas incurridos en respuesta a cualquier acto o evento que, si o cuando se revela en una publicación y visto por las partes interesadas de la compañía, podría tener un impacto adverso en la percepción pública del asegurado.
Falla del sistema	Amplía el desencadenante de la primera parte para la cobertura de interrupción de red, desde fallas de seguridad (por ejemplo, ataques) a cualquier interrupción no intencional (por ejemplo, problemas técnicos de la computadora).

CYBERSCOUT

37

Tipos de coberturas

Costo de incumplimiento de privacidad

- Legal
- Forense
- Gestión de crisis
- Notificación
- Apoyo call center
- Monitoreo de crédito
- Remediación de fraude
- Asistencia RP

Primera Parte Ciber

- Proporcionar asistencia para la restauración o recreación de datos, activos digitales
- Interrupción negocio
- Falla sistema/admin
- Fraude transferencia de fondos
- Ciberextorsión
- Eliminación de virus

Responsabilidad

- Costos de defensa y liquidación
- Multas
- Sanciones
- Seguridad red
- Responsabilidad medios
- Difamación

CYBERSCOUT

Ciberseguros Herramientas & servicios de soporte

- Monitoreo proactivo de fraude y crédito
- Educación, respuesta y remediación en casos de violación
- Servicios de resolución y gestión de identidad
- Consultoría ciberseguridad y privacidad de datos

CYBERSCOUT

Solución programa de ciberresponsabilidad para líneas comerciales y personales

CYBERSCOUT

Análisis cartera

Exposición	Análisis de su cartera de riesgo específica
Asignación grado de riesgo	Su libro de negocios categorizado por ciberriesgo
Precio	Prima compuesta ponderada: grados de peligro bajo, medio, alto

CYBERSCOUT

Grados de peligros

Bajo
- El asegurado tiene un sitio web solo con fines informativos

Medio
- El asegurado realiza negocios, al menos parcialmente, a través de su sitio web y/o números de tarjetas de crédito de la tienda, así como otra información bastante sensible

Alto
- El asegurado o bien conducirá todos sus negocios a través de su sitio web o almacenará información altamente confidencial o alguna combinación de ambos

Excluidos
- Asegurados que no son elegibles
- para un programa opt-in

CYBERSCOUT

La próxima ola de la cibercobertura: Cibercobertura personal

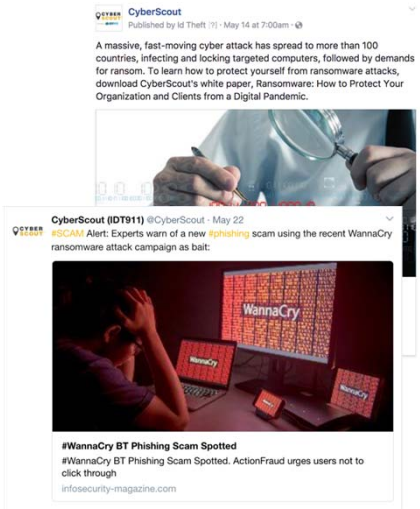
- Connected technology is reshaping the threat landscape in households.
- Even for technically savvy people, keeping up with protections against cyber threats can be a constant challenge.
- Cyber crime losses in the U.S. alone are nearly double that of property crimes – $30 billion vs. $14 billion.
- Cyber protection can help families offset financial and emotional costs of cyber crime.

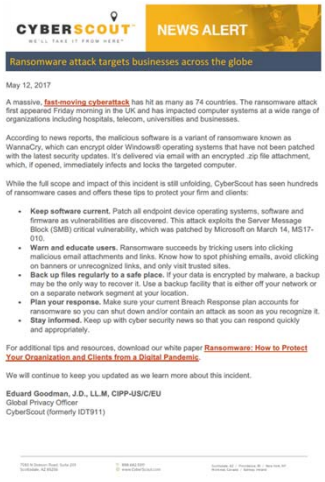
Las aseguradoras tienen la oportunidad educar y proporcionar herramientas para abordar:

- Amenazas de extorsión
- Ingeniería social
- Cyber bullying
- Robo de identidad
- Compromiso del sistema
- Limpieza de internet

CYBERSCOUT

Ejemplo: Ataque Ransomware WannaCry

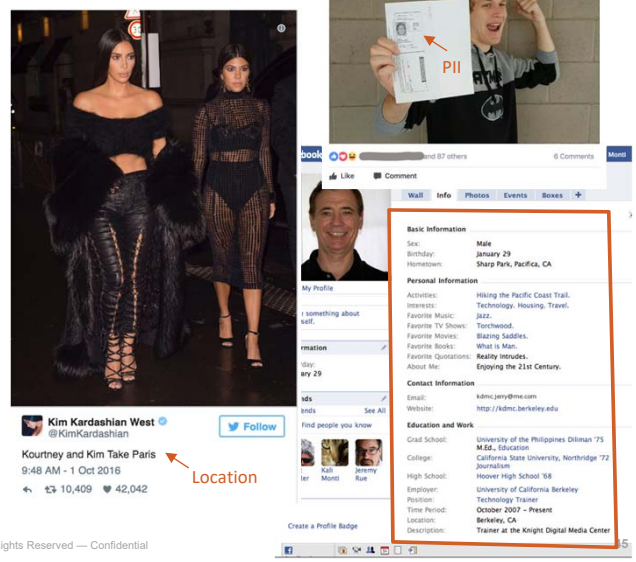




CYBERSCOUT

Practicar y enseñar buena ciberhigiene

- Eduque a los empleados sobre los riesgos cibernéticos y la importancia de la gestión de la reputación.
  - Tenga cuidado al hacer clic en anuncios o enlaces que recibe en mensajes de amigos.
  - Sepa lo que ha publicado sobre usted. Evite compartir preguntas de seguridad comunes como cumpleaños, ciudad natal, escuela secundaria, el segundo nombre de su padre, ubicación actual.
  - Sea selectivo sobre a quién acepta como amigo o conexión en una red social.
  - Tenga cuidado al instalar extras en su dispositivo o sitio, como extensiones de terceros y juegos.
  - Suponga que todo lo que pone en un sitio de redes sociales es permanente, incluso si lo elimina.



CYBERSCOUT

Involúcrese para aprender y comunicar

Minimizar	Monitorear	Gestionar
• Educar sobre los riesgos emergentes	• Responder de manera oportuna	• Inicie el Plan de Respuesta ante Crisis
• Planear contenidos sobre tendencias temporales • Impuestos, vuelta a clases, vacaciones	• Mostrar empatía	• Comunique hechos y lo que se sabe (evite especular)

• Alentar involucramiento y feedback regular	• Guiar hacia la/el persona/departamento correcto
	  • ¿Se trata de un tema de servicio al cliente?
	  • ¿Se trata de un tema de contenido?
	  • ¿Se trata de un tema de producto?
		• Refuerce consejos y educación

• Estudiar las preferencias y necesidades de los clientes	• Lleve la comunicación a un canal privado	• Considere las audiencias no en las redes sociales / canales alternativos • Email, Gacetillas, Hotline
• Mantener un ritmo regular de comunicación		• Administre el daño reputacional y busque asesoría / asistencia externa
		• Evalúe la efectividad de la respuesta

CYBERSCOUT

46

Últimos comentarios

- Los riesgos cibernéticos están comenzando a superar los riesgos tradicionales para las empresas de todo tipo y tamaño, existe una exposición global.
- Los reguladores de todo el mundo se están centrando en la privacidad del consumidor en el ámbito digital.
- La industria de seguros se ha intensificado para abordar la gestión de riesgos cibernéticos y se está extendiendo a todas las áreas.
- Las compañías de seguros corren un alto riesgo de exposición cibernética.
- Necesita un enfoque gestionado activamente para la gestión de riesgos, la respuesta y la corrección en la organización.
- Riesgo cibernético = gestión de la reputación en la era digital: si se gestiona de manera efectiva, puede proporcionar a las compañías de seguros una ventaja de mercado.

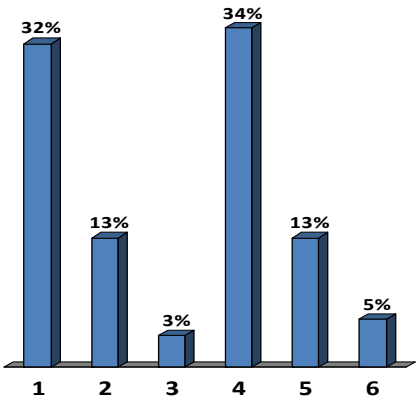
CYBERSCOUT

Q

¿Preguntas?

¿Cuán probable es que su empresa tenga un ciberataque significativo? How likely is your company to have a significant cyber attack?

1. **Ya ha sucedido** / *Has already happened*
2. **Muy poco probable** / *Very unlikely*
3. **Improbable** / *Unlikely*
4. **Probablemente** / *Likely*
5. **Muy probable** / *Very likely*
6. **No lo sé** / *I don't know*

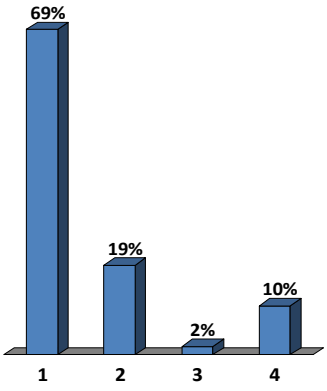


62

CYBERSCOUT

¿Su organización ha considerado ofrecer seguros cibernéticos a sus asegurados en líneas personales o comerciales? Has your organization considered offering cyber insurance to either your personal or commercial lines policyholders?

1. **no estamos considerando** / not considering
2. **estamos investigando actualmente** / currently researching
3. **lanzaremos un seguro cibernético en 2018** / we will be launching cyber insurance in 2018
4. **ofrecemos seguros cibernéticos a nuestros asegurados** / we do offer cyber insurance to our policyholders

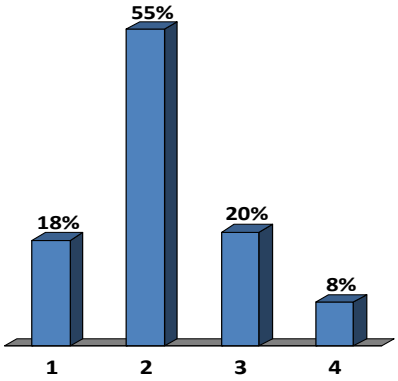


59

CYBERSCOUT

¿Como categorizaría la protección de su organización contra el riesgo cibernético? How would you categorize your organization's protection against cyber risk?

1. **muy seguro** / *very secure*
2. **algo seguro** / *somewhat secure*
3. **no muy seguro** / *not very secure*
4. **no es seguro en absoluto** / *not secure at all*



66

CYBERSCOUT

Matt Cullina | CEO
CyberScout
77 Eddy Street, 4th Floor
Providence, RI 02903

T: 401-680-4010
E: mcullina@CyberScout.com

CYBERSCOUT
WE'LL TAKE IT FROM HERE™