Riesgo cibernético en el sector de seguros

A2ii – IAIS Llamada de Consulta

26 de septiembre de 2019

Oradoras

Marcelo Ramella
Deputy Director, Financial Stability, Bermuda Monetary Authority (BMA)

Marcelo Adrián Borre
Coordinador de Evaluación Normativa, SSN, Argentina

Natalia Escobar
International Association of Insurance Supervisors (IAIS)

Regina Simoes
Iniciativa de Acceso a los Seguros (A2ii)

Temas a tratar

- Ciber riesgos – Qué son, costo de ciber ataques
- Regulación y supervisión de ciber riesgos

Temas a tratar

- Ciber riesgos – Qué son, costo de ciber ataques
- Regulación y supervisión de ciber riesgos

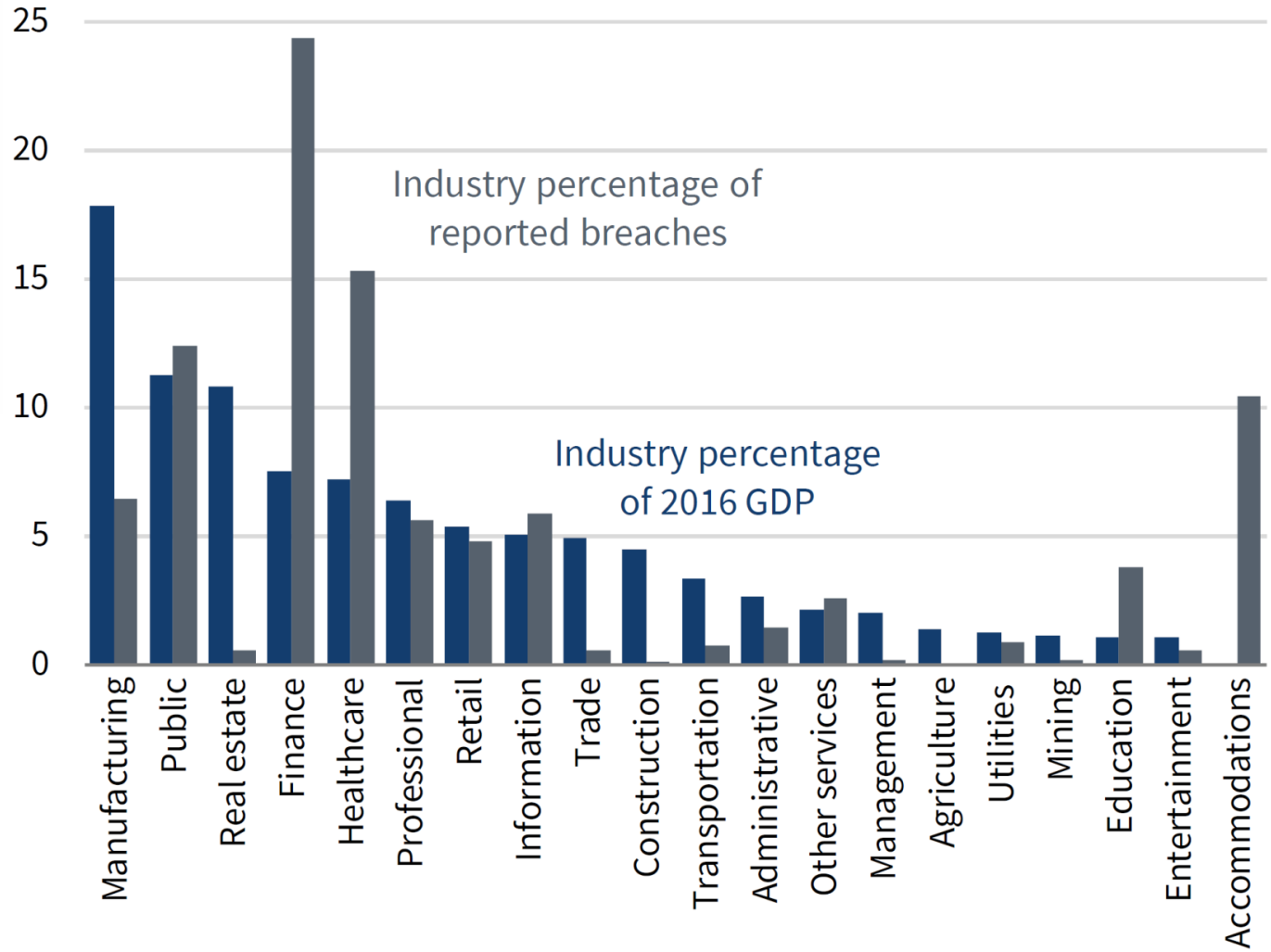
Ciber ataques y ciber riesgos

- ***Ciber ataques*** son intentos, logrados o no, de obtener acceso no autorizado a información o a sistemas de información con el objetivo de apropiarse de información, o de alterar información, o de obstruir el sistema de información
- ***Ciber riesgo*** es la combinación de probabilidad de ocurrencia de un ciber ataque con el daño que el ciber ataque haya podido causar
- Ciberataques pueden causar una multiplicidad de daños, desde interrupción en la prestación de servicios, destrucción de datos y propiedad, interrupción del negocio, robo de datos etc. hasta, potencialmente, inestabilidad financiera
- Ciberataques pueden generar considerable daño económico (costo global de ciberataques en 2018 ha sido estimado en USD800 mil millones)
- El sector financiero ha recibido comparativamente más ciberataques que otros sectores de la economía

Fuentes: FSB (2018) Cyber Lexicon. McAfee (2018) Economic Impact of Cybercrime.

BMA
BERMUDA MONETARY AUTHORITY

Ciber ataques y el sector financiero

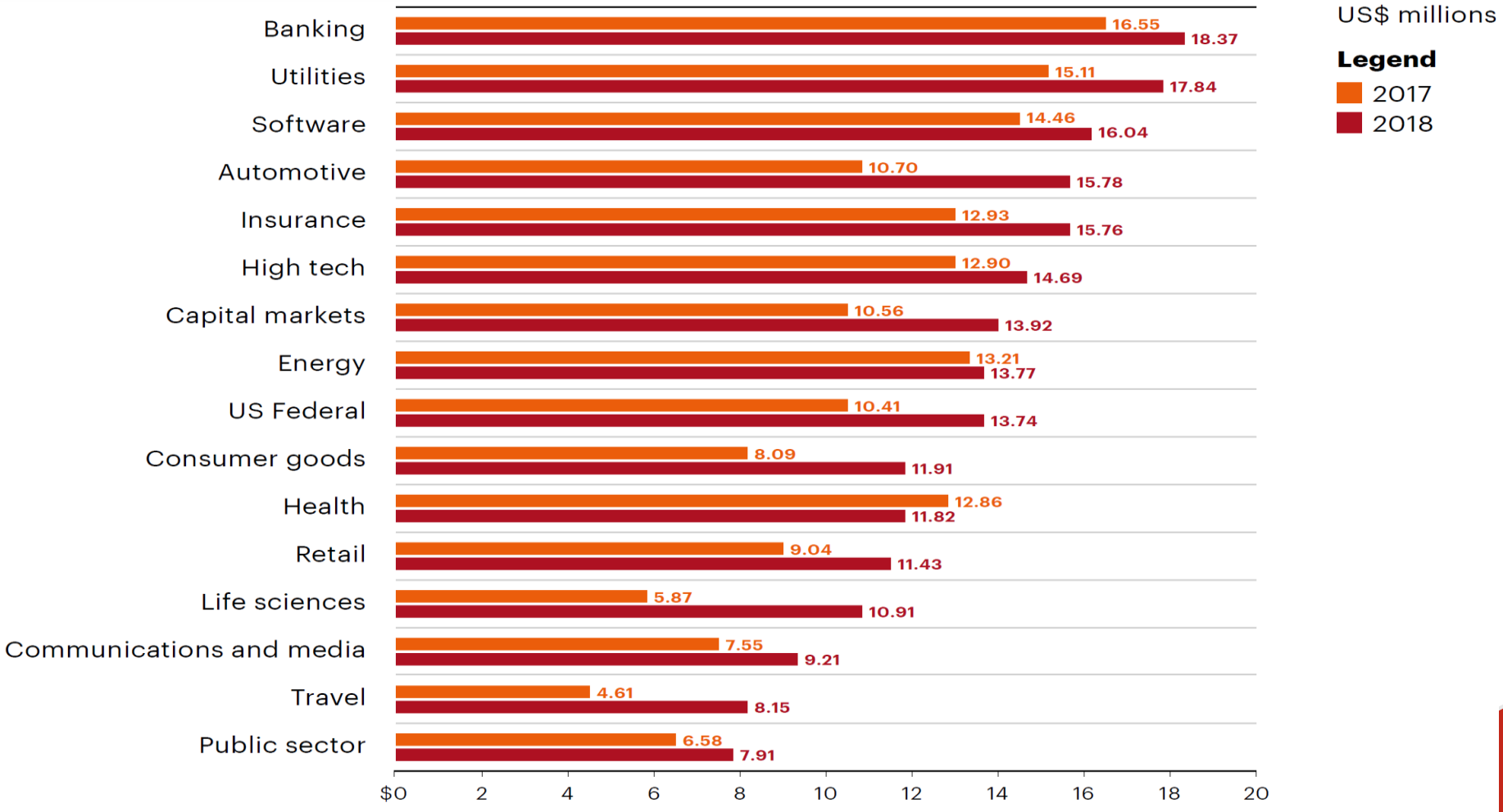


Fuente:
The Council of Economic Advisers (2018) The cost of malicious cyber activity to the U.S. economy.

BMA
BERMUDA MONETARY AUTHORITY

Ciber ataques – Daño económico

Costo anual promedio de ciber ataques por sector

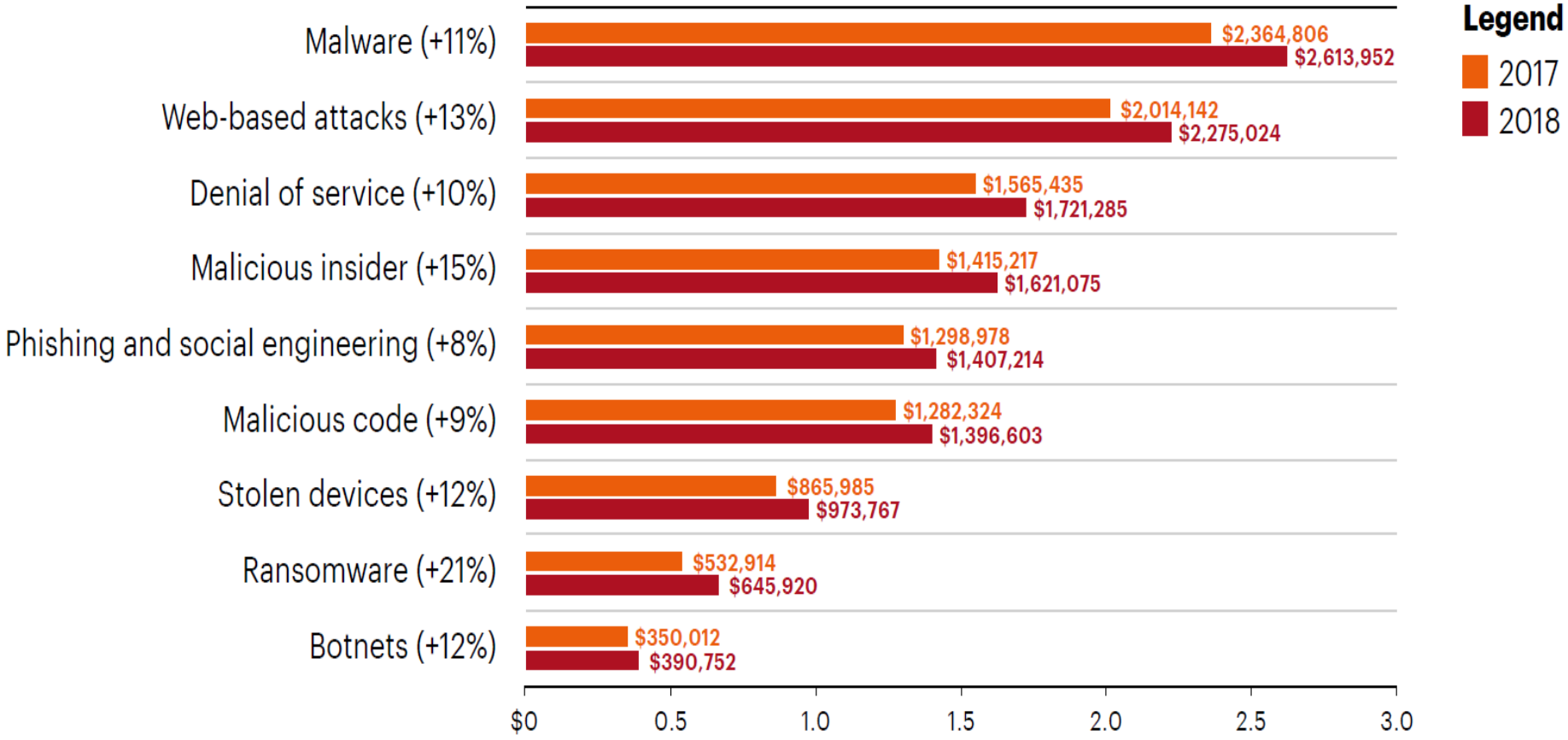


Fuente: Accenture (2019) The cost of cyber crime

BMA
BERMUDA MONETARY AUTHORITY

Ciber ataques – Daño económico

Costo anual promedio de ciber ataques por tipo de ataque

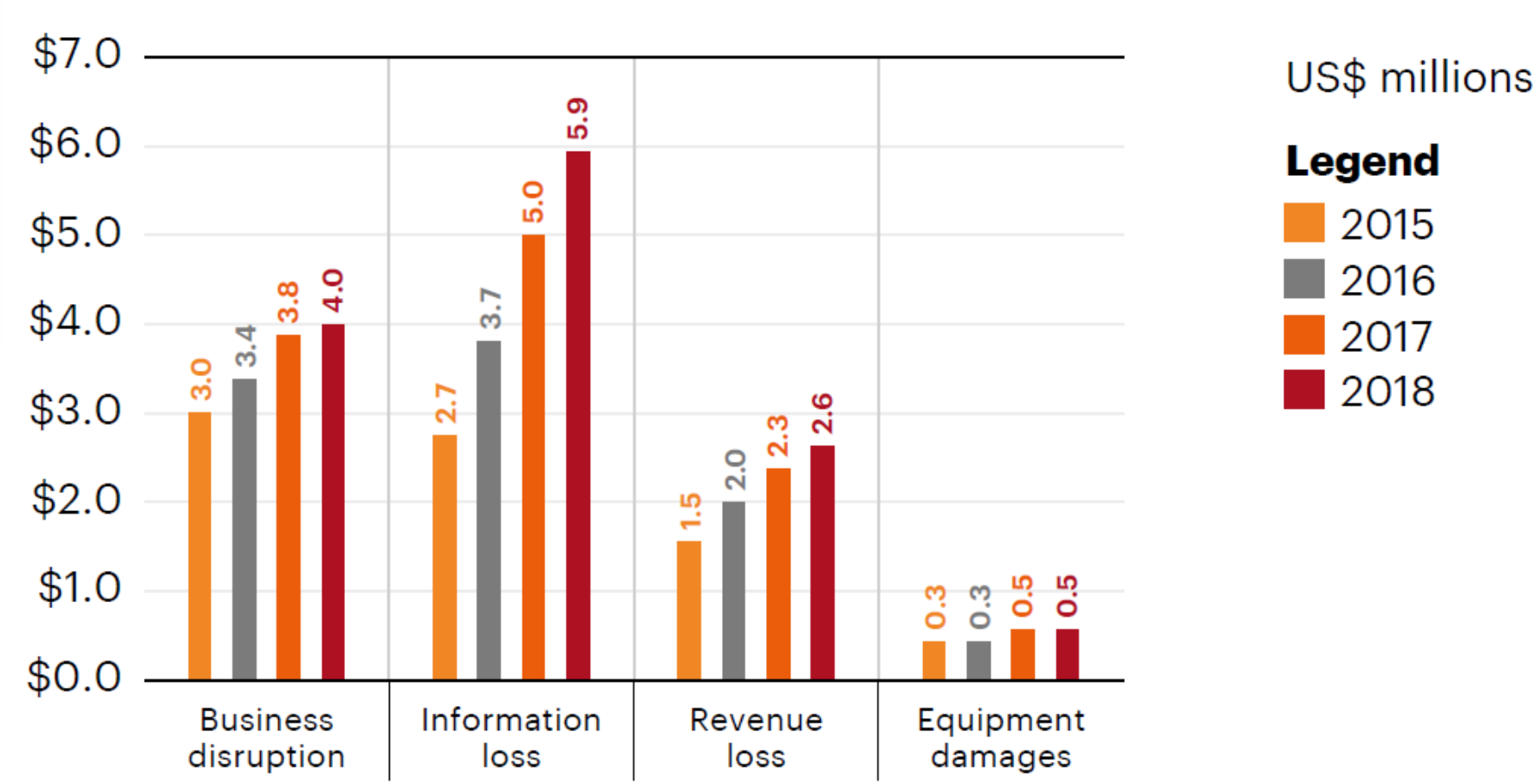


Fuente: Accenture (2019) The cost of cyber crime

BMA
BERMUDA MONETARY AUTHORITY

Ciber ataques – Daño económico

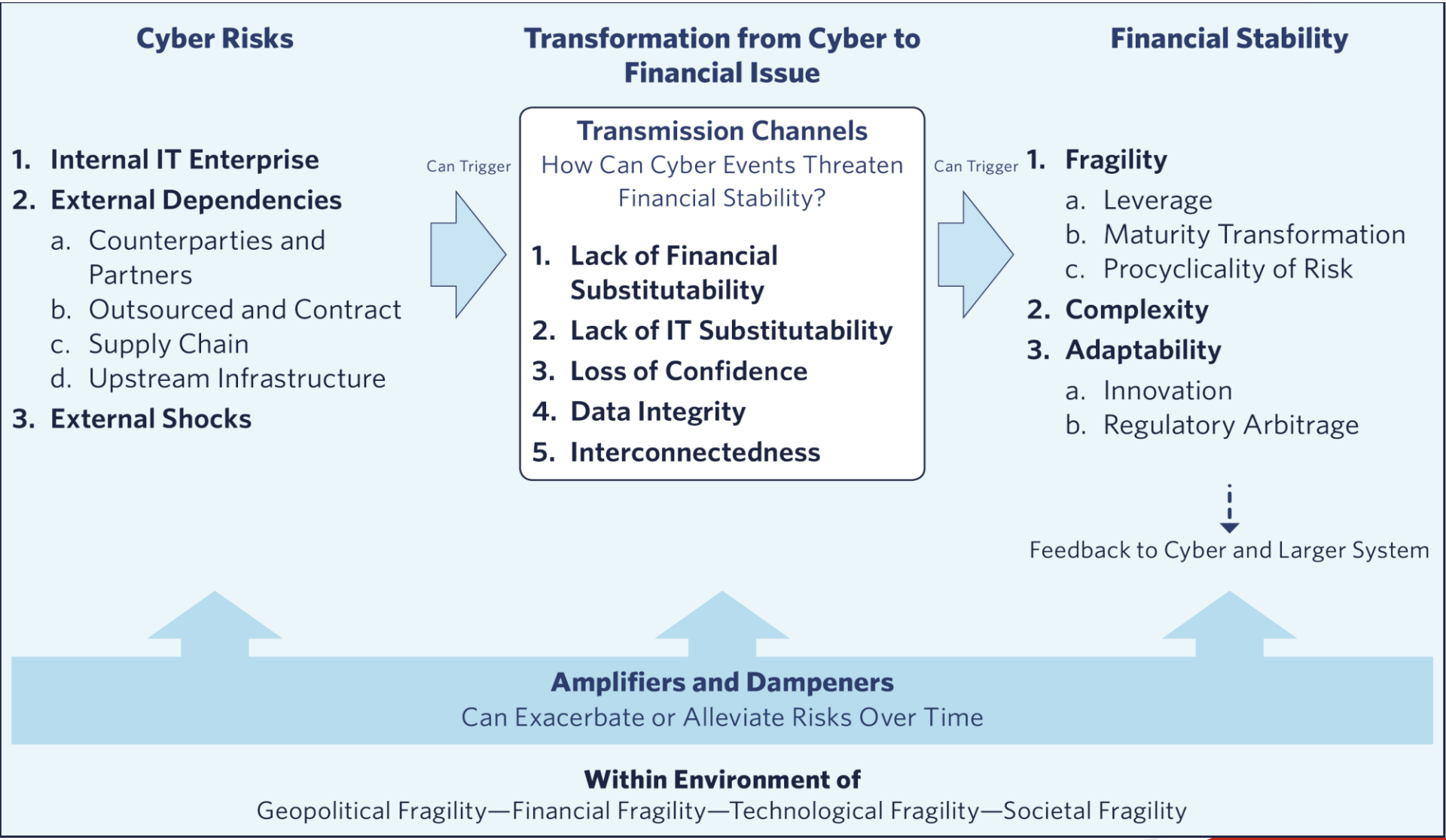
Costo anual promedio de ciber ataques por consecuencia del ataque



Fuente: Accenture (2019) The cost of cyber crime

BMA
BERMUDA MONETARY AUTHORITY

Ciber ataques y estabilidad financiera



Fuente: Healy, J. et al. (2018) The Ties that Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability, Columbia SIPA. December 2018.

BMA
BERMUDA MONETARY AUTHORITY

Temas a tratar

- Regulación y supervisión de ciber riesgos

- Regulación y supervisión de ciber riesgos

G7 - Elementos Fundamentales de seguridad cibernética

- Breve documento (tres páginas) articulando los elementos fundamentales de la gestión de los ciber riesgos a considerar por las entidades públicas - ***incluídos supervisores de seguros*** - y privadas del sector financiero

- Los ocho elementos fundamentales identificados por el G7 son:
  1. ***Estrategia y marco de seguridad cibernética***
  2. ***Gobernanza***
  3. ***Evaluación de riesgos y control***
  4. ***Supervisión***
  5. ***Respuesta***
  6. ***Recuperación***
  7. ***Intercambio de información***
  8. ***Aprendizaje continuo***

Fuente: G7 (2016) Fundamental Elements of Cybersecurity

BMA
BERMUDA MONETARY AUTHORITY

G7 - Elementos Fundamentales de seguridad cibernética - evaluación

- Breve documento (cinco páginas) producido por el G7 en 2017 y que acompaña los ocho elementos fundamentales (G7FE)

- Propone como evaluar los elementos fundamentales del G-7 articulando un conjunto de:

  – ***resultados deseables (Parte A),*** y

  – un proceso para su ***evaluación y revisión (Parte B)***

Fuente:

G7 (2017) G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector.

BMA
BERMUDA MONETARY AUTHORITY

Riesgos ciber y la IAIS

Issues Paper on Cyber Risk to the Insurance Sector (agosto de 2016):

- Producido con el objetivo de crear conciencia entre aseguradores y supervisores de los desafíos presentados por el riesgo cibernético, incluidos los enfoques de supervisión actuales y contemplados para abordar estos riesgos
- Presenta y debate antecedentes, describe prácticas actuales, identifica ejemplos y explora cuestiones y desafíos relacionados con la regulación y la supervisión del riesgo ciber en las aseguradoras

Application Paper on Supervision of Insurer Cybersecurity (noviembre de 2018):

- Presenta lineamientos guía para supervisores interesados en desarrollar o fortalecer sus marcos de supervisión de riesgos ciber
- Analiza en detalle los ocho elementes fundamentales elaborados por el G7 y como se relacionan con los PBS de IAIS
- Elabora ejemplos de marcos en vigor en autoridades de supervisión miembros de IAIS

BMA
BERMUDA MONETARY AUTHORITY

Seguridad cibernética y PBSs

G7FE 1 - Estrategia y marco de seguridad cibernética

- Las aseguradoras debe especificar como identifica, gestiona y reduce sus ciber riesgos en modo integrado y exhaustivo

- El **PBS 8.1** exige al supervisor que requiera a las aseguradoras que establezcan sistemas efectivos de gestión de riesgos y de controles internos, y que funcione dentro de ese marco
  - Riesgos a la ***capacidad de la aseguradora de operar*** sin problemas y riesgo a la ***información sobre los asegurados*** en poder de la aseguradora

- Ejemplos de controles
  - Hay una estrategia y un marco explícitos y claros?
  - Influyen en las decisiones de la aseguradora? Se usan en la práctica?
  - Están sujetos a revisión? Cuando fue la última revisión?

BMA
BERMUDA MONETARY AUTHORITY

Seguridad cibernética y PBSs (cont.)

G7FE 2 - Gobernanza

- Las aseguradoras debe definir roles y responsabilidades del personal encargado de implementar, gestionar y supervisar la ejecución de la estrategia de ciberseguridad. Las aseguradoras deben proveer los recursos necesarios para la ejecución de la estrategia de ciberseguridad

- El **PBS 7** exige al supervisor que requiera a las aseguradoras que establezcan e implementen un marco de gobierno corporativo que brinde una administración y supervisión de la actividad de la aseguradora estable y prudente, y que reconozca y proteja de manera adecuada los intereses de los asegurados

- Ejemplos de controles
  - Cual es el grado y frecuencia de participación del Consejo de Administración en asuntos de ciberseguridad de la aseguradora? Y de la alta gerencia?
  - Hay políticas y procedimientos claros? Se aplican?
  - Hay recursos suficientes para llevar a cabo las políticas?
  - Cual es el presupuesto de ciberseguridad?

BMA
BERMUDA MONETARY AUTHORITY

Seguridad cibernética y PBSs (cont.)

G7FE 3 - Evaluación de riesgos y control

- Las aseguradoras debe identificar funciones, actividades y servicios (incluidos servicios tercerizados) sujetos a ciber riesgos, entender y evaluar los riesgos, e implementar los controles correspondientes. Estos últimos deben ser consistentes con el apetito de riesgo de la aseguradora

- El **PBS 8** exige al supervisor que requiera a las aseguradoras que cuenten con sistemas efectivos de gestión de riesgos y controles internos, incluyendo funciones eficaces en materia de gestión de riesgos

- El **PBS 19.12** exige al supervisor que requiera a las aseguradoras y a los intermediaros que tengan políticas y procedimientos para la protección y uso de información sobre los consumidores
- Ejemplos de controles
  - Cual es el grado de conocimineto de la aseguradora de sus ciber riesgos? Hay un registro de ciber riesgos? Se usa? Está actualizado?
  - Es ciber riesgo parte del perfil de riesgo general de la aseguradora?
  - Grado de protección de la información sobre los consumidores

BMA
BERMUDA MONETARY AUTHORITY

Seguridad cibernética y PBSs (cont.)

G7FE 4 - Supervisión

- Las aseguradoras deben tener sistemas de monitoreo que permitan ***detectar ciber ataques rápidamente***. Las aseguradoras deben permanentemente evaluar la ***efectividad de los controles*** en existencia sobre los ciber riesgos, incluídos simulacros de ciber ataques

- El **PBS 8.1** exige al supervisor que requiera a las aseguradoras que establezcan sistemas efectivos de gestión de riesgos, incluidos sistemas de alerta temprana y respuesta a la materialización de riesgos

- El **PBS 8.2** exige al supervisor que requiera a las aseguradoras que los sistemas de monitoreo estén sujetos periodicamante a pruebas de efectividad

- Ejemplos de controles
  - Hay sistemas de monitoreo permanente de actividades de alto riesgo (p.e. acceso a información confidencial)? Es el monitoreo en tiempo real?
  - Qué está siendo monitoreado (p.e. hardware y software a riesgo)?
  - Hay evidencia de simulacros llevados a cabo por la aseguradora?
  - Qué uso ha tenido el resultado del simulacro?

BMA
BERMUDA MONETARY AUTHORITY

Seguridad cibernética y PBSs (cont.)

G7FEs 5 y 6 – Respuesta y recuperación

- Las aseguradoras deben responder a ciber ataques oportunamente, entendiendo la seriedad del ataque, conteniendo sus efectos, notificando apropiadamente a quien corresponda, y coordinando y ejecutando una respuesta que les permita volver a operar normalmente

- El **PBS 8.1.2** establece los elementos necesarios que las aseguradoras deben considerar para poder responder a la materialización de riesgos en modo efectivo y proporcional al riesgo que se ha materializado
- Ejemplos de controles
  - Qué políticas y procedimientos existen en la aseguradora para promover concientización sobre ciber riesgos (p.e. programas de capacitación del personal sobre ciber riesgos)?
  - Hay planes explícitos que detallen como responder a ataques?
  - Hay planes explícitos que detallen como volver a operar normalmente?
  - Hay políticas y procedimientos de notificacion de ciber ataques?
  - Qué investigaciones llevó a cabo la aseguradora luego de un ciber ataque?

BMA
BERMUDA MONETARY AUTHORITY

Seguridad cibernética y PBSs (cont.)

G7FEs 7 – Intercambio de información

- Las aseguradoras deben informar sobre amenazas, vulnerabilidades, ataques, y respuestas a ataques con el objetivo de mejorar respuestas a ataques, limitar daños, concientizar y promover aprendizaje. Las aseguradores deben informar internamente y externamente, incluyendo a autoridades públicas
- El PBS 8.1.2 (en especial, el tema de planificación de contingencias) y el PBS 16.10 (gestión de riesgo empresarial) proveen el sustento normativo a los supervisores para exigir a las aseguradoras que informen sobre sus sistemas de gestión de ciber riesgos así como también sobre la materialización de riesgos
- Los PBS 3, PBS 25 y PBS 26 tratan el tema de intercambio de información entre supervisores así como también la cooperación entre supervisores, incluyendo cooperación en la gestión de crisis internacionales
- Ejemplos de controles

– Participa la aseguradora de grupos especializados de intercambio de informacion sobre ciber riesgos?

– Comparte la aseguradora informacion sobre ciber riesgos con proveedores de servicios tercerizados?

BMA
BERMUDA MONETARY AUTHORITY

Seguridad cibernética y PBSs (cont.)

G7FEs 8 – Aprendizaje continuo

- Las aseguradoras deben mantener sus sistemas de gestión de riesgos ciber constantemente bajo revisión con el objetivo de mantenerlos actualizados con respecto a nuevos ciber riesgos y también con el objetivo de brindarles los recursos adecuados

- El **PBS 16.10** (gestión de riesgo empresarial) exige al supervisor que requiera a las aseguradoras incorporen un circuito de retroalimentación que permita tomar medidas necesarias en forma oportuna como respuesta a los cambios surgidos en el propio perfil de riesgo

- Ejemplos de controles
  - Hay indicaciones de la existencia de un circuito de retroalimentación en los sistemas de gestión de ciber riesgos de la aseguradora? De ser asi, hay evidenca que tal circuito este funcionando efectivamente (p.e. esta siendo utilizado?)?
  - Con que frecuencia de revisa/actualizan los sistemas de gestión de ciber riesgos? Cuán exhaustivas son las revisiones?

BMA
BERMUDA MONETARY AUTHORITY

Muchas gracias

Follow us on Twitter @a2ii_org, Youtube and LinkedIn

Marcelo Ramella
Deputy Director
Financial Stability
Bermuda Monetary Authority
www.bma.bm
mramella@bma.bm
+1 441 278 0218 (direct)
+1 441 304 3031 (mobile)

BMA
BERMUDA MONETARY AUTHORITY

Mesa de Innovación en Seguros

INSURTECH ARG 2019

Riesgo cibernético en el sector de seguros

A2ii-IAIS Llamada de Consulta

SSN | SUPERINTENDENCIA DE SEGUROS DE LA NACIÓN

Ministerio de Hacienda
Presidencia de la Nación

Mesa de Innovación en Seguros e Insurtech

¿Qué es?

Evento Seminario Regional para Supervisores de Seguros, organizado por IAIS, FSI, BIS
Junto al XV Foro Consultivo sobre Seguros Inclusivos organizado por A2ii, IAIS, MiN

Se gesta la creación Mesa de innovación (resolución 733/2019)

Mesa de Innovación en Seguros

¿Qué busca?

Aprovechar los avances tecnológicos para modernizar el sector asegurador en pos de brindar un mejor servicio a los asegurados o mejorar sus propios procesos.

Tecnología

Brindar oportunidades de desarrollo a **proyectos que presenten soluciones** con tecnología aplicada a la industria aseguradora.

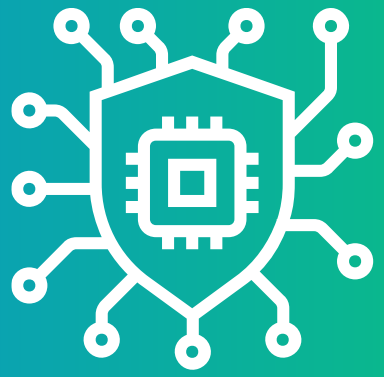
Seguros

Generar un **ambiente de intercambio y discusión** para encontrar soluciones colaborativas a problemas específicos del sector.

SSN

Impulsar modificaciones normativas para **acompañar la innovación, protegiendo al asegurado.**

Mesa de Innovación en Seguros
Cyber Risk



Grupo de Trabajo

Cyber Risk

Miembros

- **Aseguradoras líderes** en materia de seguridad cibernética
- **Proveedores de Servicios** de Seguridad Informática
  (Big Techs – Software Companies)
- Especialistas y Consultores en Cyber Risk
- Staff SSN
- Staff Ministerio de Modernización
- Staff Ministerio de Seguridad

Objetivos

A. **Documento consolidado de Manual de Tecnologías de Información del Sector Asegurador** con buenas prácticas de gestión de riesgos y recursos de IT.

B. **Medidas para Prevenir y Perseguir Crímenes** de Delito Informático (Min. Seguridad)

C. Elaborar **medidas que mejoren oferta**, asistencia tecnológica

D. **Colaborar** con proveedores de servicios digitales de Cybersecurity para fortalecer industria.

Mesa de Innovación en Seguros

Cyber Risk

+210

Aseguradoras y Reaseguradoras en Argentina, de características heterogéneas.

Regulación

Que contemple los diferentes espectros de grado de avance tecnológico, los ICP's y el Application Paper de IAIS.

Mesa de Innovación en Seguros

INSURTECH ARG 2019

¡Muchas gracias!

Contacto:
mesadeinnovacion@ssn.gob.ar

ssn_ar

ssn_arg

SSN | SUPERINTENDENCIA DE SEGUROS DE LA NACIÓN

Ministerio de Hacienda
Presidencia de la Nación