Les risques de piratage informatique dans le secteur des assurances

A2ii – IAIS Consultation téléphonique

26 septembre 2019

Présentatrices

Expert technique

Andrea Camargo
Director, Inspowering
Expert technique, A2ii

Modérateur

Mariella Regh
Access to Insurance Initiative (A2ii)

Sujets à aborder

- Risques de piratage informatique: ce qu'ils sont, ce qu’ils coûtent
- Réglementation et contrôle des risques informatiques

BMA
BERMUDA MONETARY AUTHORITY

Sujets à aborder

- Risques de piratage informatique: ce qu'ils sont, ce qu’ils coûtent
- Réglementation et contrôle des risques informatiques

BMA
BERMUDA MONETARY AUTHORITY

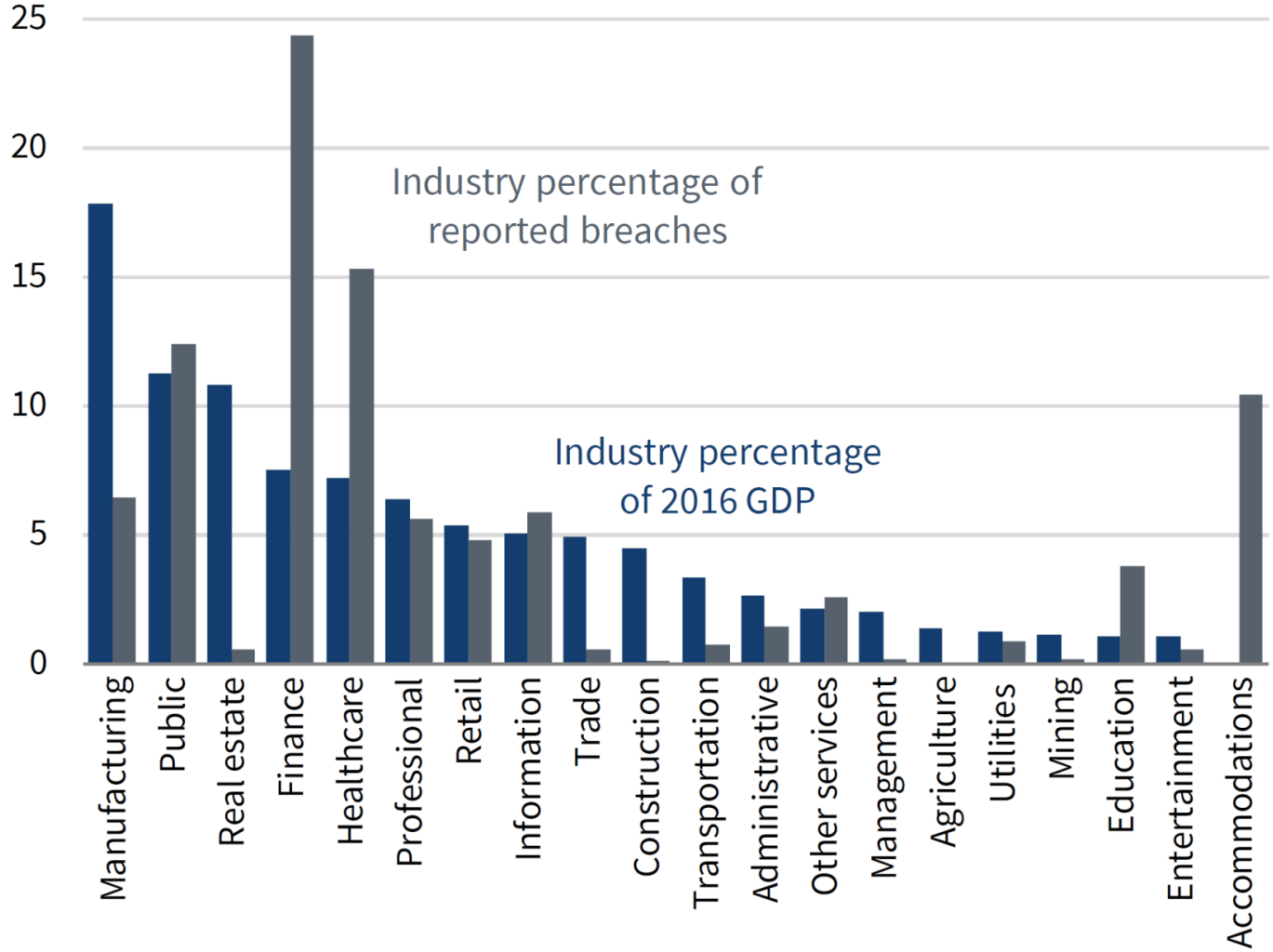
Attaques informatiques et risques de piratage informatique

- Les ***actes de piratage informatique*** sont des tentatives, réussies ou avortées, d'obtenir l'accès non autorisé à des données ou à des systèmes informatiques, dans le but de dérober ou de modifier des informations, ou encore de bloquer des systèmes.
- Les ***risques de de piratage informatique*** sont la combinaison entre la probabilité d'une attaque et les dommages qu'elle peut causer
- Les attaques informatiques peuvent causer un large éventail de dommages: interruptions de services; destruction de données et de biens ; perturbation des activités, vol de données, etc. et peuvent aller jusqu'à causer une instabilité financière.
- Les attaques informatiques peuvent générer des dommages économiques considérables (leur coût global en 2018 était estimé à 800 milliards USD).
- Le secteur financier a subi relativement plus d'attaques informatiques que les autres secteurs économiques

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

BMA
BERMUDA MONETARY AUTHORITY

Le piratage informatique dans le secteur financier

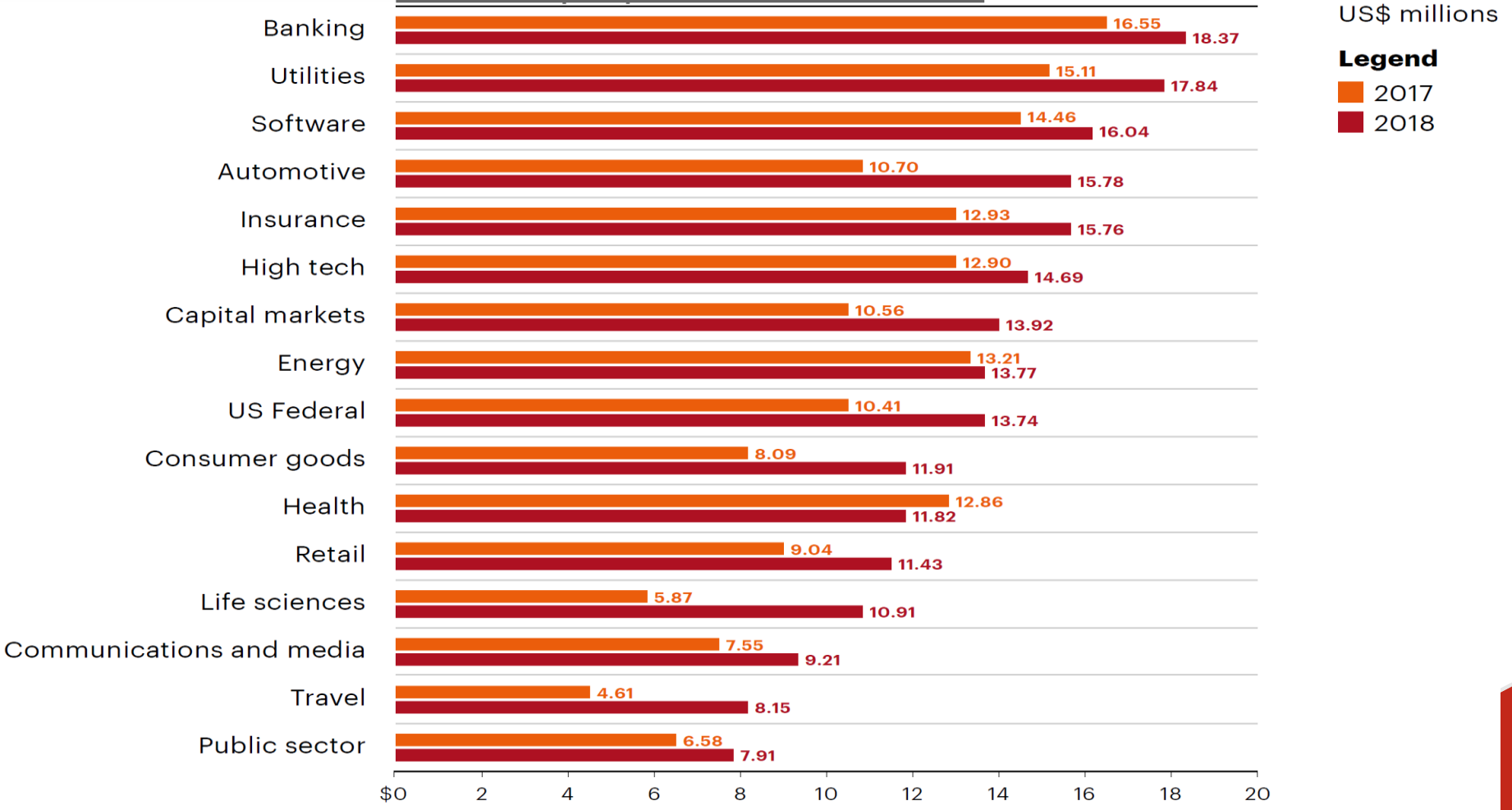


Source:
The Council of Economic Advisers (2018) The cost of malicious cyber activity to the U.S. economy.

BMA
BERMUDA MONETARY AUTHORITY

Actes de piratage informatique: les dommages économiques

Coûts annuels moyens des actes de piratage informatique par secteur d'activité

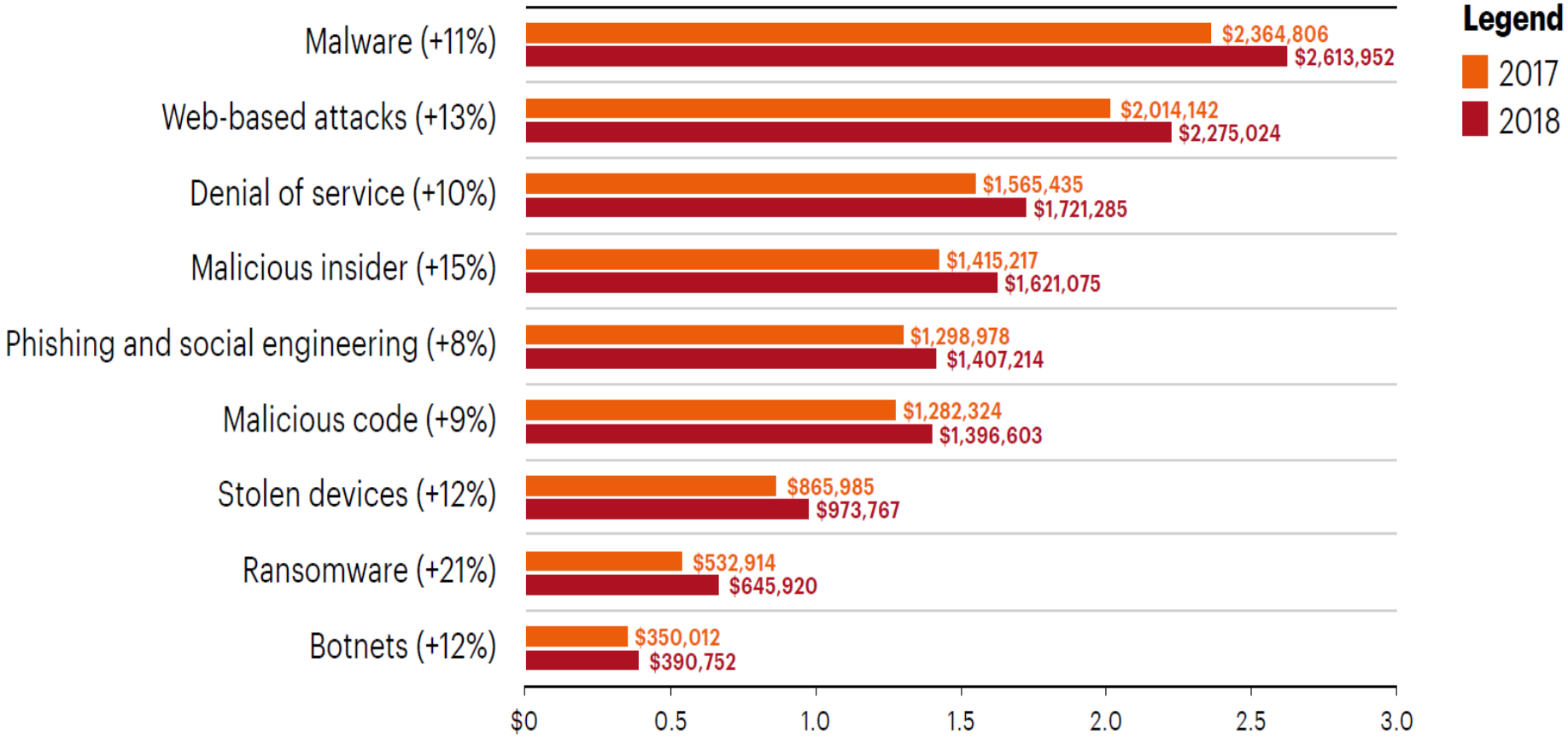


Source: Accenture (2019) The cost of cyber crime

BMA
BERMUDA MONETARY AUTHORITY

Actes de piratage informatique: les dommages économiques

Coûts annuels moyens des attaques informatiques par type d'acte de piratage

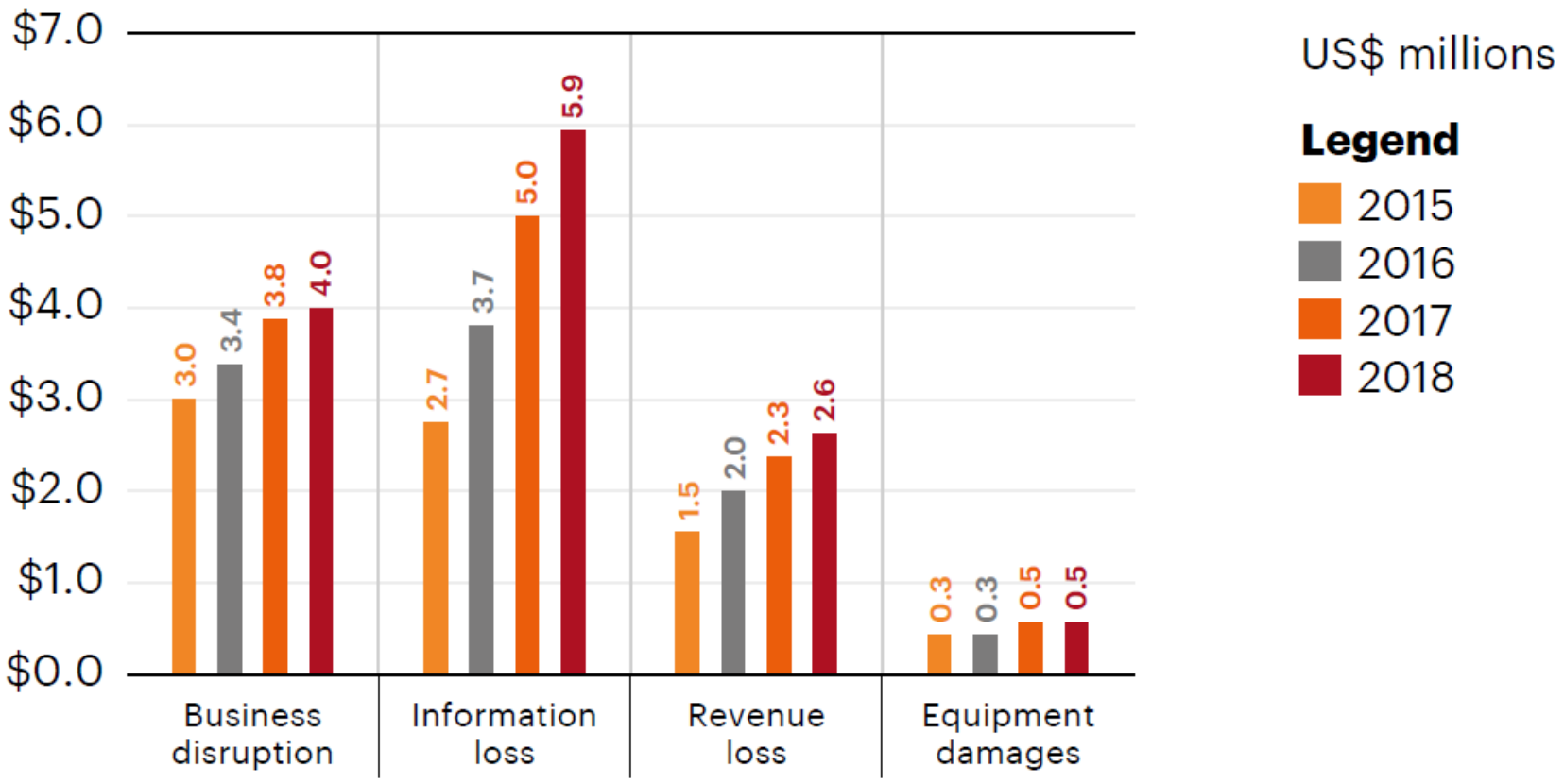


Source: Accenture (2019) The cost of cyber crime

BMA
BERMUDA MONETARY AUTHORITY

Actes de piratage informatique: les dommages économiques

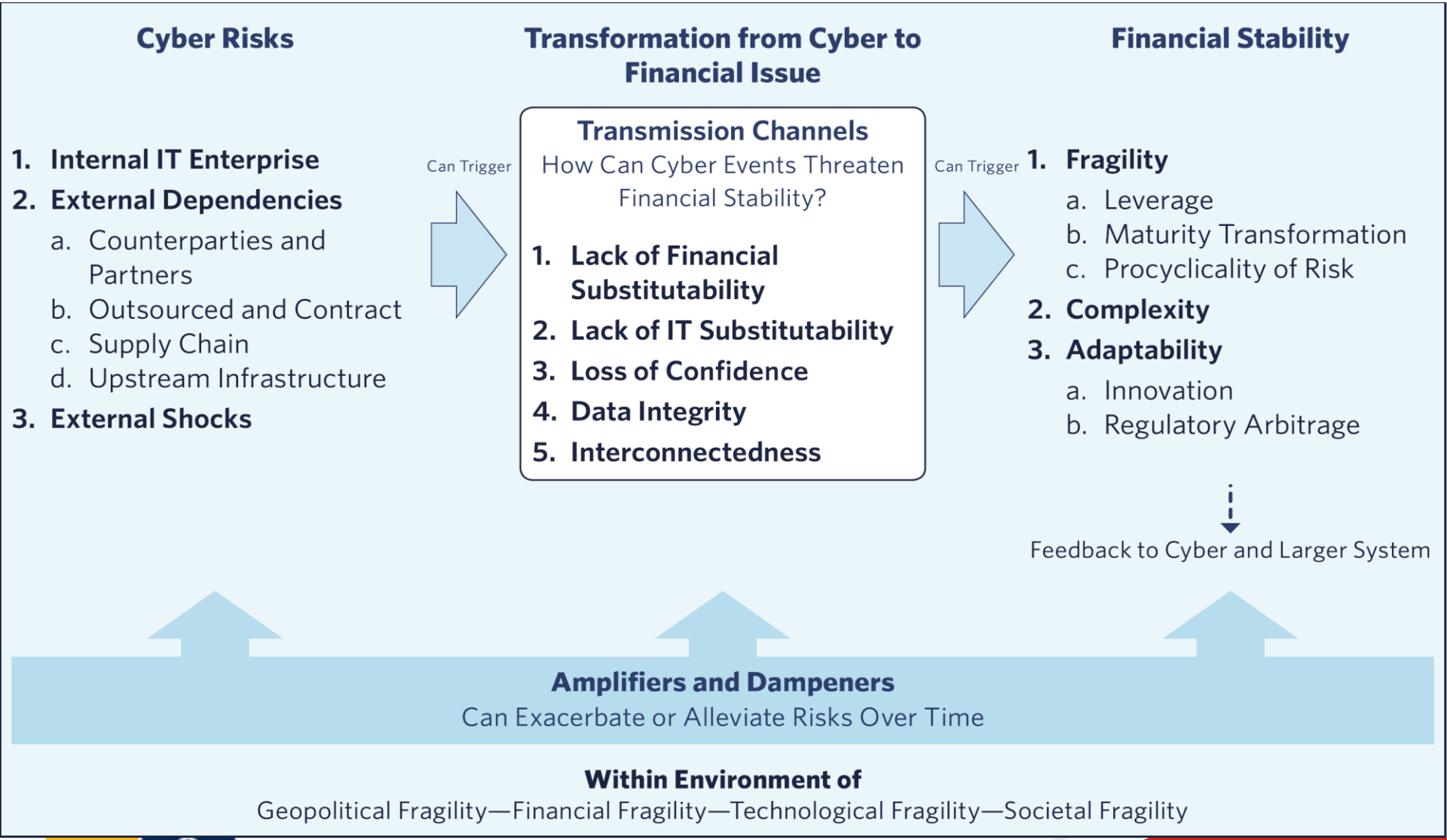
Coûts annuels moyens des actes de piratage informatique par conséquences de l'acte de piratage



Source: Accenture (2019) The cost of cyber crime

BMA
BERMUDA MONETARY AUTHORITY

Actes de piratage informatique et stabilité financière



Source: 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.

Topics to be Addressed

- Risques de piratage informatique: ce qu'ils sont, ce qu'ils coûtent
- Réglementation et contrôle des risques de piratage informatique

G7 - Éléments fondamentaux de la sécurité informatique

- Une synthèse de trois pages énumérant les éléments fondamentaux de la gestion des risques informatiques dont les entités privées et publiques doivent prendre en compte ***- y compris les contrôleurs d'assurance -*** dans le secteur financier

- Les huit éléments fondamentaux identifiés par le G7 sont:
  1. ***Stratégie et cadre en matière de sécurité informatique***
  2. ***Gouvernance***
  3. ***Évaluation et maîtrise des risques***
  4. ***Surveillance***
  5. ***Réaction***
  6. ***Reprise des activités***
  7. ***Partage d'information***
  8. ***Apprentissage continu***

Source:

G7 (2016) Fundamental Elements of Cybersecurity

BMA
BERMUDA MONETARY AUTHORITY

G7 - Éléments fondamentaux de la sécurité informatique - Évaluation

- Une synthèse de cinq pages préparée par le G7 en 2017, qui accompagne les huit éléments fondamentaux (G7FE)

- Le document propose des méthodes d'évaluation des éléments fondamentaux du G-7 en recherchant ***des résultats souhaitables (partie A),*** ainsi que le processus nécessaire à leur **évaluation et examen (partie B)**

Source:

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

BMA
BERMUDA MONETARY AUTHORITY

Les risques informatiques et l'AICA

Document de synthèse sur les risques de piratage informatique pour le secteur des assurances (Août 2016).

- Produit dans le but de sensibiliser les assureurs et les contrôleurs aux défis que posent les risques de piratage informatique, en particulier les approches actuelles en matière de contrôle et celles envisagées pour contrer cette catégorie de risque
- Présenter et discuter des aspects généraux, décrire les pratiques actuelles, trouver des exemples et explorer les problèmes et les défis liés aux risques de piratage informatique, à la réglementation et au contrôle des assureurs

Document de mise en œuvre sur la maîtrise de la sécurité informatique auprès des assureurs (Novembre 2018)

- Présente des directives aux contrôleurs souhaitant développer ou renforcer leurs cadres de surveillance autour des risques informatiques
- Analyse détaillée des huit éléments fondamentaux du G7 et de leur lien avec les PBA de l'AICA
- Énumérer des exemples de cadres d'autorité de surveillance en vigueur parmi les membres de l'AICA

BMA
BERMUDA MONETARY AUTHORITY

Sécurité informatique et PBA

G7FE 1 - Stratégie et encadrement de la sécurité informatique

- Les assureurs doivent indiquer comment identifier, traiter= et réduire leurs risques de piratage informatique de façon intégrée et exhaustive.

- **PBA 8.1** appelle les autorités de contrôle à demander aux assureurs de mettre en place des systèmes efficaces de gestion des risques et de contrôle interne, fonctionnant dans ce cadre
  - Risques pour la capacité opérationnelle de l'assureur et risques pour les renseignements sur les titulaires de police détenues par l'assureur

- Exemples de mesures de contrôle
  - Existe-t-il une stratégie et un cadre clairs et explicites?
  - Influencent-ils les décisions des assureurs? Sont-ils utilisés dans la pratique?
  - Sont-ils parfois révisés ? À quand remonte la dernière révision?

BMA
BERMUDA MONETARY AUTHORITY

Sécurité informatique et PBA (suite)

G7FE 2 - Gouvernance

- Les assureurs doivent définir les ***rôles et responsabilités*** du personnel chargé de mettre en œuvre, gérer et superviser la mise en œuvre de la stratégie de sécurité informatique. Les assureurs doivent fournir toutes les ressources nécessaires pour mettre en œuvre la stratégie de sécurité informatique.
- Le **PBA 7** demande aux autorités de contrôle d'imposer aux assureurs d'établir et de mettre en œuvre des cadres de gouvernement d'entreprise qui sous-tendent une administration et un contrôle stable et prudente de leurs activités et qui reconnaissent et protègent adéquatement les intérêts des assurés.
- Exemples de mesures de contrôle
  - Dans quelle mesure et à quelle fréquence le conseil d'administration participe-t-il aux enjeux du piratage informatique auprès des assureurs? Et qu'en est-il de la haute direction?
  - Existe-t-il des politiques et procédures clairement définies? Sont-elles vraiment mise en œuvre?
  - Y a-t-il suffisamment de ressources pour pouvoir mettre en œuvre les politiques?
  - Quel est le budget consacré à la sécurité informatique?

BMA
BERMUDA MONETARY AUTHORITY

Sécurité informatique et PBA (suite)

G7FE 3 - Évaluation des risques et des mesure de contrôles

- Les assureurs doivent être en mesure d'identifier les fonctions, activités et services (y compris les services externalisés) sujets aux risques de piratage informatique, les comprendre et les évaluer afin de pouvoir mettre en œuvre les mesures de contrôles adéquates. Ces mesures doit être proportionnées au degré de prise de risque de l'assureur.

- Le **PBA 8** demande aux autorités de contrôle d'imposer aux assureurs de travailler avec des systèmes internes de contrôle et de gestion des risques, notamment des responsabilités de gestion des risques.

- Le **PBA19.12** demande aux autorités de contrôle d'imposer aux assureurs et aux courtiers de disposer de politiques et de procédures encadrant la protection et des données des consommateurs et leur utilisation.

- Exemples de mesures de contrôle
  - Quel est le degré de connaissances de l'assureur sur ses propres risques de subir un piratage informatique? Existe-t-il un registre des risques de piratage informatique? Est-il utilisé? Est-il régulièrement actualisé?
  - Le risque de piratage informatique est-il intégré au profil de risque général de l'assureur?
  - Degré de protection des données des consommateurs

BMA
BERMUDA MONETARY AUTHORITY

Sécurité informatique et PBA (suite)

G7FE 4 - Contrôle

- Les assureurs doivent disposer de systèmes de surveillance leur permettant de ***détecter rapidement les actes de piratage informatique***. Les assureurs doivent évaluer en permanence l'efficacité de leurs mesures de contrôle effectives pour contrer les risques de piratage informatique, notamment en effectuant des simulations d'attaques.
- Le **PBA 8.1** appelle les autorités de contrôle à demander aux assureurs de mettre en place des systèmes efficaces de gestion des risques, y compris des systèmes d'alerte précoce et de réaction aux risques
- Le **PBA 8.2** appelle les autorités de contrôle à demander aux assureurs dotés de systèmes de surveillance de réaliser régulièrement des tests d'efficacité
- Exemples de mesures de contrôle
  - Existe-t-il des systèmes de surveillance en continu des activités à haut risque (notamment sur l'accès aux données confidentielles)? La surveillance est-elle effectuée en temps réel?
  - Qu'est-ce qui fait l'objet d'une surveillance (par exemple, le matériel et les logiciels à risque)?
  - Existe-t-il un registres des simulations effectuées par l'assureur?
  - Comment les résultats des simulations sont-ils utilisés?

BMA
BERMUDA MONETARY AUTHORITY

Sécurité informatique et PBA (suite)

G7FEs 5 et 6 - Réaction et reprise des activités

- Les assureurs doivent réagir promptement aux actes de piratage informatique, être conscients de la gravité de l'attaque, en limiter les effets, émettre les notifications adéquates à qui de droit, et coordonner et mettre en œuvre des réponses leur permettant de reprendre leurs activités normales.
- Le **PBA 8.1.2** définit les éléments nécessaires que les assureurs doivent prendre en compte afin de réagir efficacement et proportionnellement à la matérialisation des risques.
- Exemples de mesures de contrôle
  - Quelles sont les politiques et procédures en vigueur chez les assureurs pour mieux faire connaître les risques de piratage informatique (p. ex.: des programmes de renforcement des capacités du personnel axés sur les risques de piratage informatique)?
  - **E**xiste-t-il des plans explicites assortis de descriptions détaillées sur la manière de réagir à ce type d'attaques?
  - **E**xiste-t-il des plans explicites expliquant en détail comment revenir à un fonctionnement normal des activités ?
  - **E**xiste-t-il des politiques et des procédures de notification en cas d'acte de piratage informatique ?
  - Quelles enquêtes ont été menées par l'assureur à la suite d'un acte de piratage informatique?

BMA
BERMUDA MONETARY AUTHORITY

Sécurité informatique et PBA (suite)

G7FEs 7 – Partage de renseignements

- Les assureurs doivent fournir des informations sur les menaces, les faiblesses, les attaques et les réaction aux attaques afin d'améliorer la qualité de la riposte, limiter les dommages, renforcer le niveau de sensibilisation et promouvoir l'apprentissage interne. Les assureurs doivent informer en interne, mais aussi à l'externe, notamment en notifiant les autorités.
- Les **PBA 8.1.2** en particulier le sujet de la planification d'urgence et **PBA 16.10** (gestion des risques de l'entreprise) fournissent un soutien réglementaire aux contrôleurs qui demandent aux assureurs de les informer sur leurs systèmes de gestion des risques informatiques, ainsi que sur la matérialisation de ces risques.
- Les **PBA 3, 25 et 26** traitent de la question de l'échange d'informations entre autorités de contrôle, ainsi que de leur coopération, notamment en matière de gestion des crises internationales.
- Exemples de mesures de contrôle
  - L'assureur appartient-il à des groupes spécialisés qui échangent des informations sur les risques de piratage informatique?
  - L'assureur partage-t-il les informations sur les risques de piratage informatique avec des prestataires de services externalisés?

BMA
BERMUDA MONETARY AUTHORITY

Sécurité informatique et PBA (suite)

G7FEs 8 - Apprentissage continu

- Les assureurs doivent surveiller en permanence leurs systèmes de gestion des risques de piratage informatique afin de s'adapter aux nouveaux risques de piratage informatique tout en leur fournissant les ressources adéquates.

- Le **PBA 16.10** (gestion des risques de l'entreprise) demande aux autorités de contrôle d'imposer aux assureurs l'inclusion d'un circuit de rétroaction leur permettant de prendre les mesures nécessaires en temps utile, en réponse aux modifications du profil de risque

- Exemples de mesures de contrôle
  - Existe-t-il des indications sur l'existence de circuits de rétroaction dans les systèmes de gestion des risques de piratage informatique des assureurs? Dans l'affirmative, existe-t-il des preuves que ces circuits fonctionnent efficacement (sont-ils utilisés)?
  - À quelle fréquence les systèmes de gestion des risques sont-ils revus / mis à jour? À quel point ces examen sont-ils exhaustifs?

BMA
BERMUDA MONETARY AUTHORITY

Merci!

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