Cyber Risk in the Insurance Sector

A2ii – IAIS Consultation Call

26 September 2019

Expert

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

Supervisory Presenter

Jennifer McAdam
Senior Counsel, National Association of Insurance Commissioners (NAIC)

IAIS representative

Alessandro Nardi
International Association of Insurance Supervisors (IAIS)

Moderator

Janina Voss
Access to Insurance Initiative (A2ii)

Topics to be Addressed

- Cyber risks – what they are, costs of cyber attacks
- Regulation and supervision of cyber risks

BMA
BERMUDA MONETARY AUTHORITY

Topics to be Addressed

- Cyber risks – what they are, costs of cyber attacks
- Regulation and supervision of cyber risks

BMA
BERMUDA MONETARY AUTHORITY

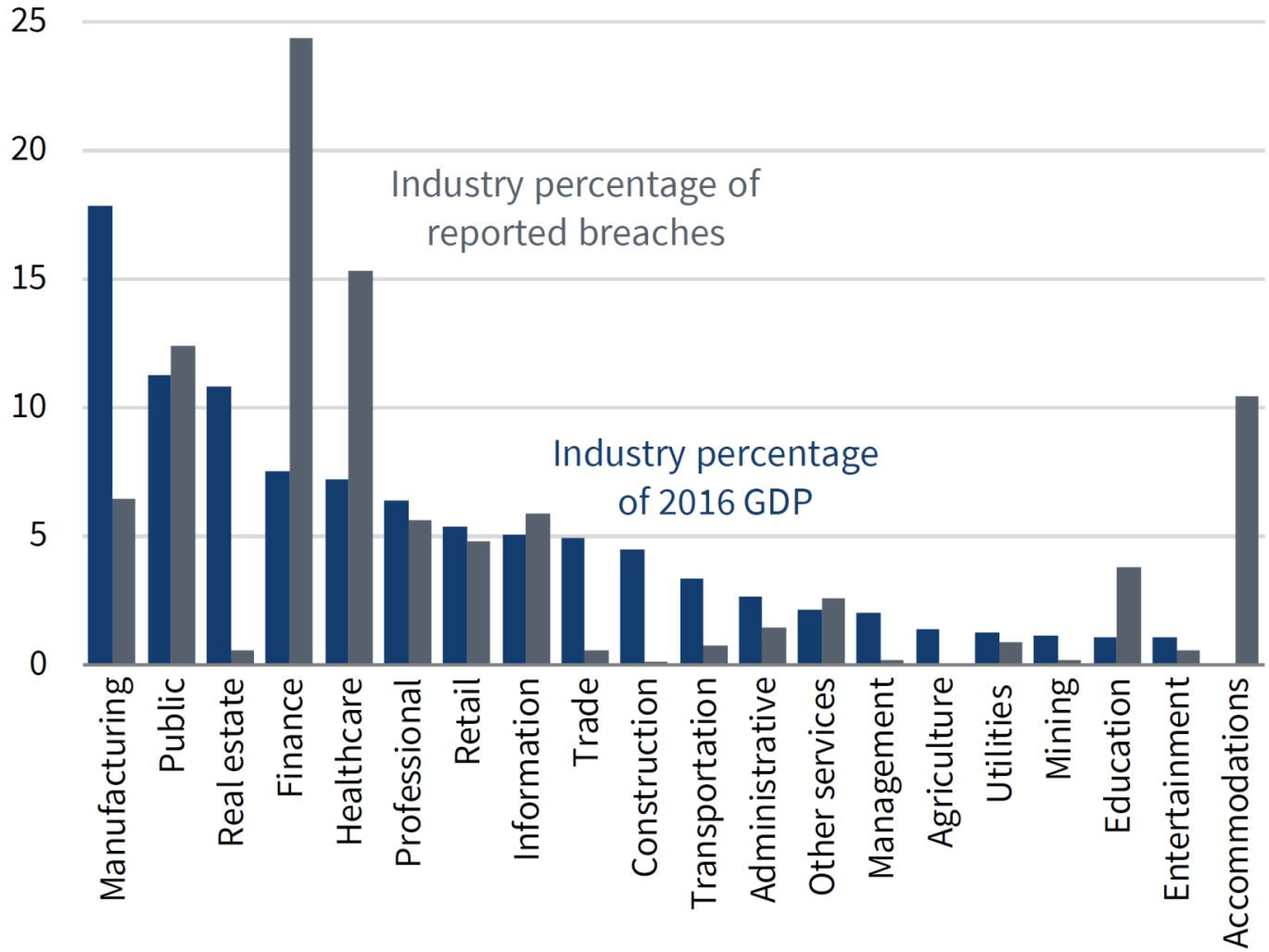
Cyber Attacks and Cyber Risks

- ***Cyber attacks*** are attempts, successful or not, to obtain unauthorised access to information or information systems, in order to steal or alter information or block information systems.
- ***Cyber risk*** is the combination of the probability of a cyber attack occurring, with the damages that a cyber attack may have caused
- Cyber attacks may cause a broad range of damages, ranging from interruptions in services through to the destruction of data and property, as well as business disruptions, data theft, etc. up to potential financial instability
- Cyber attacks may generate considerable economic damage (the global costs of cyber attacks in 2018 were estimated at USD 800 billion)
- The financial sector has received comparatively more cyber attacks than other economic sectors

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

BMA
BERMUDA MONETARY AUTHORITY

Cyber Attacks and the Financial Sector

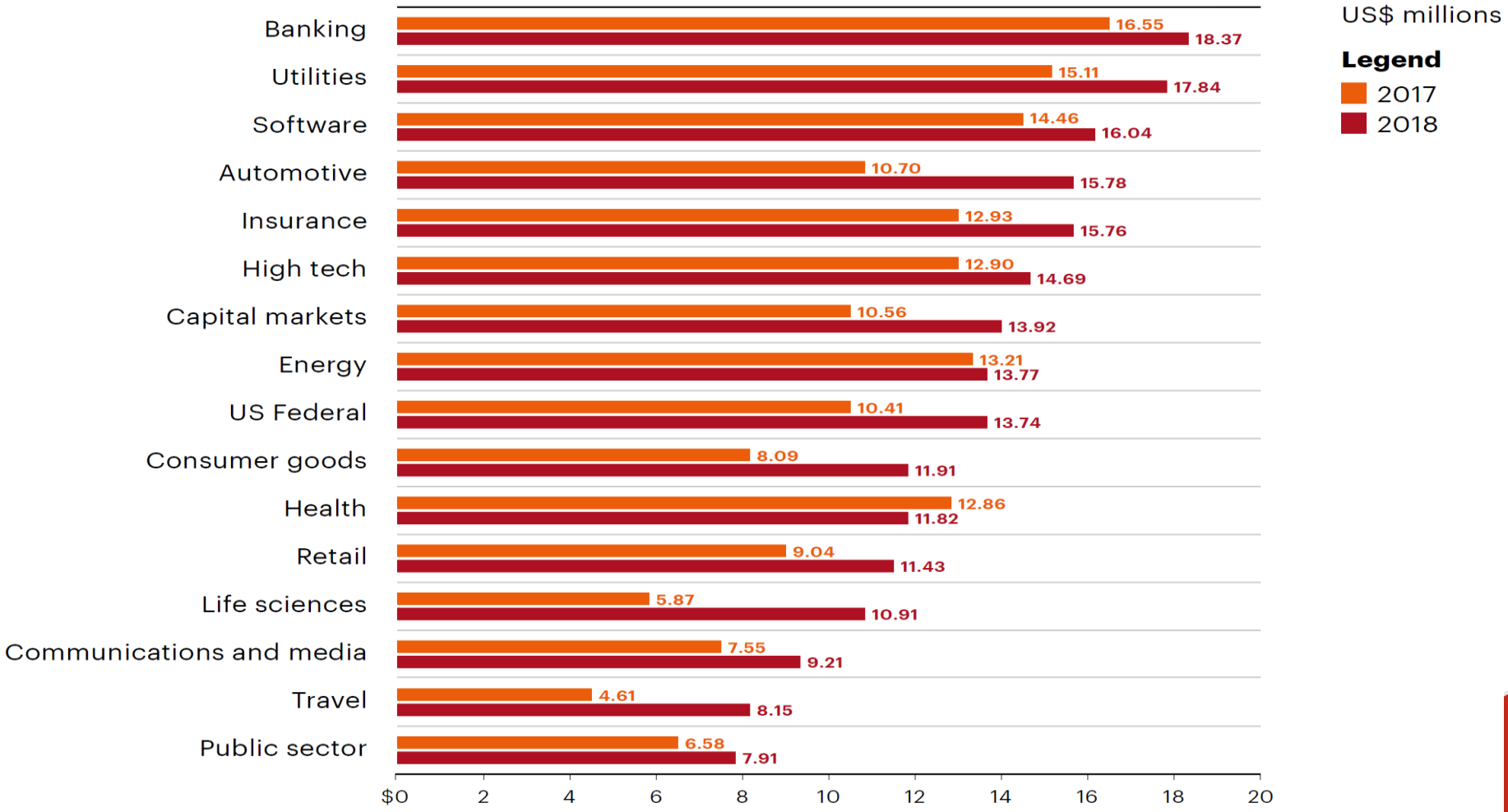


Source:
The Council of Economic Advisers (2018) The cost of malicious cyber activity to the U.S. economy.

BMA
BERMUDA MONETARY AUTHORITY

Cyber Attacks – Economic Damage

Mean Annual Costs of Cyber Attacks by Sector

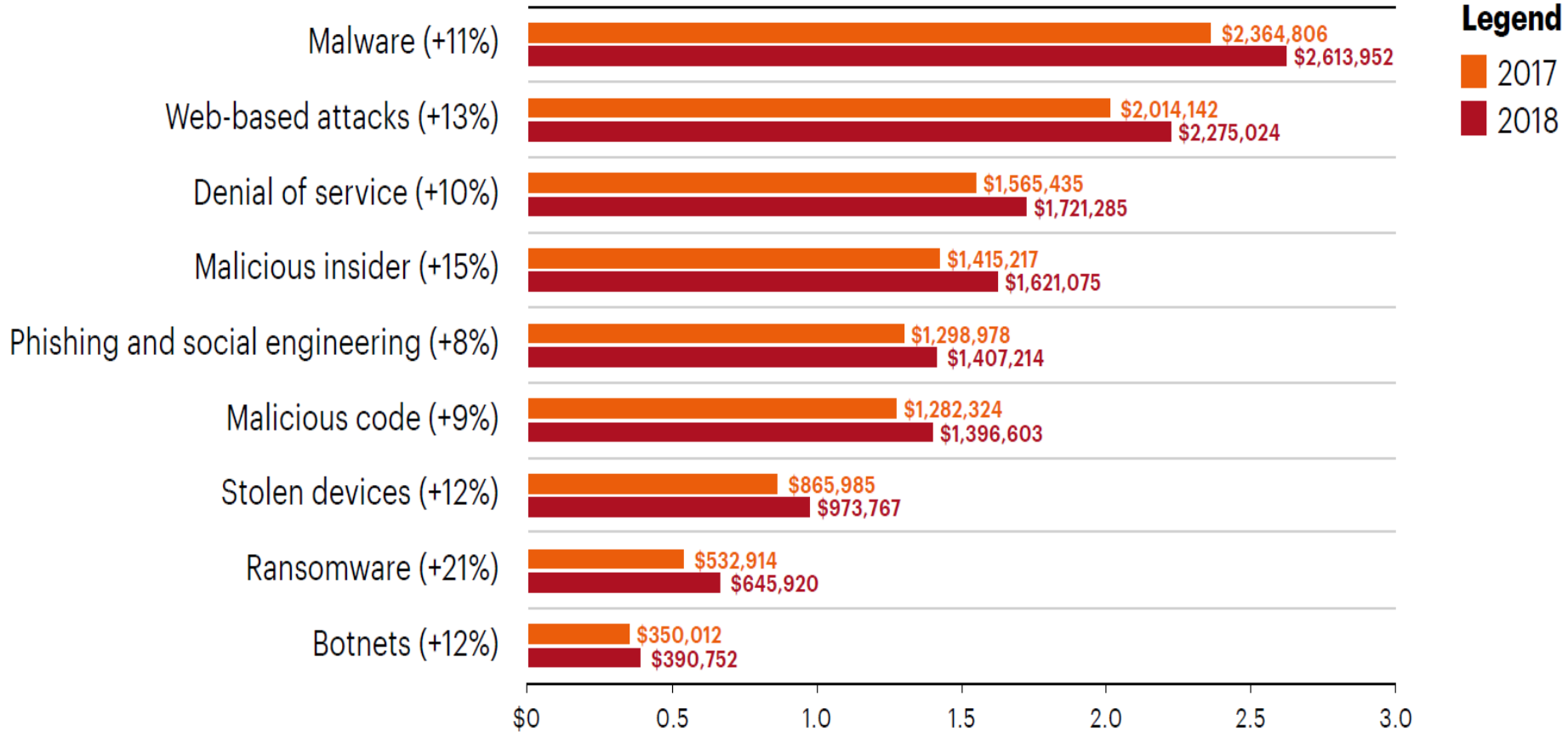


Source: Accenture (2019) The cost of cyber crime

BMA
BERMUDA MONETARY AUTHORITY

Cyber Attacks – Economic Damage

Mean Annual Costs of Cyber Attacks by Type of Attack

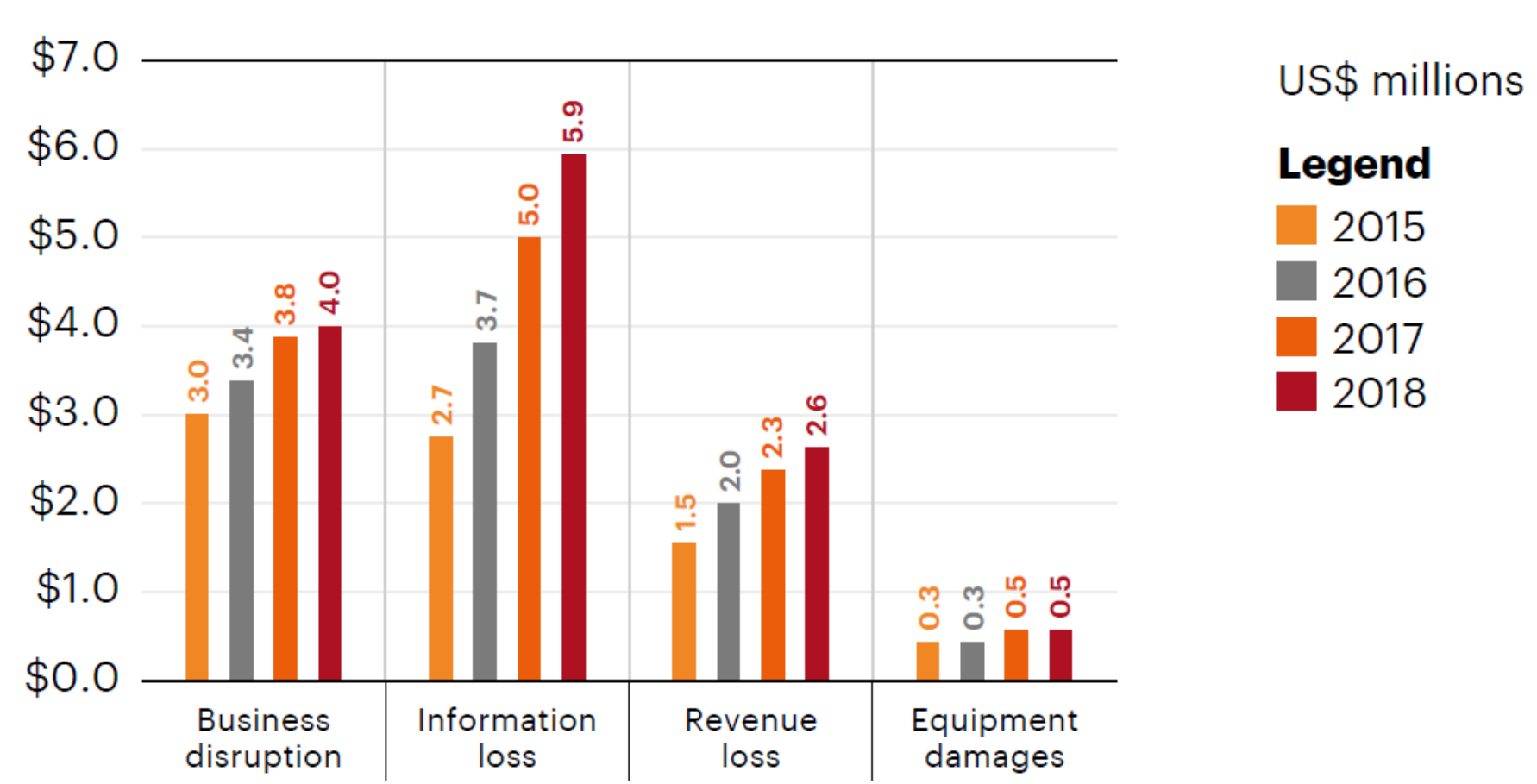


Source: Accenture (2019) The cost of cyber crime

BMA
BERMUDA MONETARY AUTHORITY

Cyber Attacks – Economic Damage

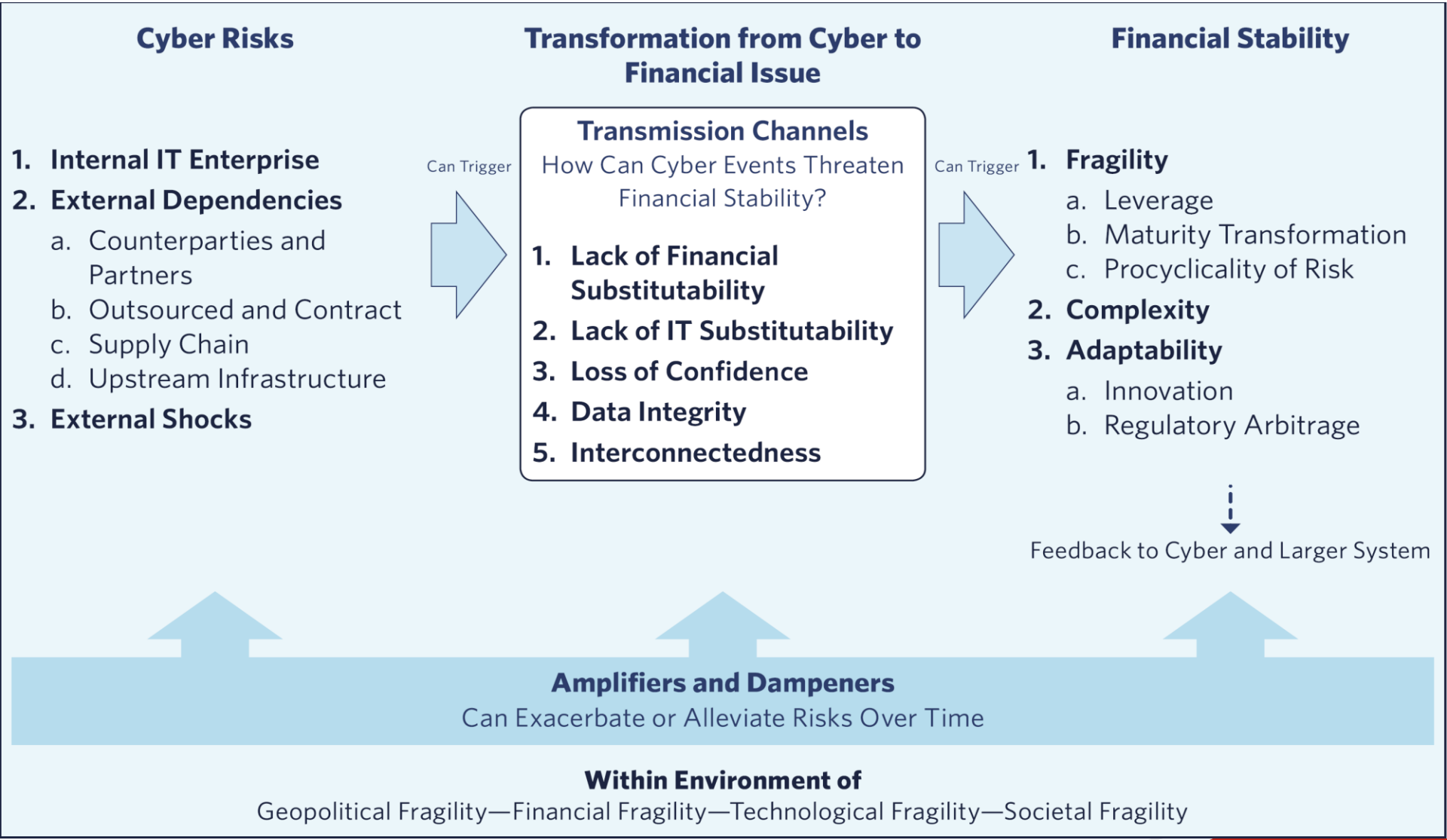
Mean Annual Costs of Cyber Attacks by Consequences of the Attack



Source: Accenture (2019) The cost of cyber crime

BMA
BERMUDA MONETARY AUTHORITY

Cyber Attacks and Financial Stability



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.

BMA
BERMUDA MONETARY AUTHORITY

Topics to be Addressed

- Cyber risks – what they are, costs of cyber attacks
- Regulation and supervision of cyber risks

BMA
BERMUDA MONETARY AUTHORITY

G7 - Fundamental Elements of Cybersecurity

- A brief (three-page) document listing the fundamental elements for managing cyber risks to be taken into consideration by private and public entities **– *including insurance supervisors*** - in the financial sector

- The eight fundamental elements identified by the G7 are:
  1. ***Cybersecurity Strategy and Framework***
  2. ***Governance***
  3. ***Risk and Control Assessment***
  4. ***Supervision***
  5. ***Response***
  6. ***Recovery***
  7. ***Information sharing***
  8. ***Continuous learning***

Source:

G7 (2016) Fundamental Elements of Cybersecurity

BMA
BERMUDA MONETARY AUTHORITY

G7 - Fundamental Elements of Cybersecurity – Evaluation

- A brief (five-page) document prepared by the G7 in 2017, that accompanies the eight fundamental elements (G7FE)

- It proposes how to assess the G-7 fundamental elements, through pursuing a set of:

  – ***Desirable Outcomes (Part A),*** and

  – a process for their ***Assessment and Review (Part B)***

Source:

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

BMA
BERMUDA MONETARY AUTHORITY

Cyber Risks and the IAIS

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

- Produced in order to heighten awareness among insurers and supervisors of the challenges raised by cyber risks, including current supervision approaches and others under consideration for addressing these risks
- Presents and discusses background aspects, describing current practices, identifying examples and exploring issues and challenges related to cyber risk and regulation and supervision of insurers

Application Paper on Supervision of Insurer Cybersecurity (November 2018):

- Presents guidelines for supervisors wishing to develop or strengthen their cyber risks supervision frameworks
- Detailed analysis of the eight G7 fundamental elements and how they are related to the IAIS ICPs
- List examples of supervision authority frameworks in effect among IAIS members

BMA
BERMUDA MONETARY AUTHORITY

Cybersecurity and ICPs

G7FE 1 – Cybersecurity strategy and framework

- Insurers must specify how to identify, manage and reduce their cyber risks in an integrated and exhaustive manner

- **ICP 8.1** calls for supervisors to require insurers to set up effective risk management and internal control systems, that function within this framework
  - Risks to the ***insurer operating capability*** without problems and risks to ***policy holder information*** held by the insurer

- Examples of Controls
  - Is there a clear and express strategy and framework?
  - Do they influence insurer decisions? Are they used in practice?
  - Are they subject to review? When was the last review?

BMA
BERMUDA MONETARY AUTHORITY

Cybersecurity and ICPs (cont.)

G7FE 2 - Governance

- Insurers must define the ***roles and responsibilities*** of staff required to implement, manage and supervise the implementation of cybersecurity strategy. Insurers must provide the ***necessary resources*** to implement the cybersecurity strategy.

- **ICP 7** calls for supervisors to require insurers to establish and implement corporate governance frameworks that underpin stable and prudent administration and supervision of insurer activities, and that acknowledge and protect policy holder interests adequately.

- Examples of Controls
  - What is the level and frequency of Board participation in cybersecurity matters among insurers? And senior management?
  - Are there clear policies and procedures? Are they applied?
  - Are there sufficient resources to implement policies?
  - What is the cybersecurity budget?

BMA
BERMUDA MONETARY AUTHORITY

Cybersecurity and ICPs (cont.)

G7FE 3 - Evaluation of risks and controls

- Insurers must identify functions, activities and services (including outsourced services) subject to cyber risks, understanding and assessing risks and implementing the corresponding controls. The latter must be aligned with the risk appetite of the insurer.

- **ICP 8** calls for supervisors to require insurers to work with internal control and risk management systems, including efficacious risk management functions.

- **ICP 19.12** calls for supervisors to require insurers and brokers to have policies and procedures in place for the protection and use of consumer information.

- Examples of Controls
  - What is the insurer's level of knowledge of their cyber risks? Is there a cyber risks record? Is it used? Is it updated?
  - Is cyber risk part of the general risk profile of the insurer?
  - Level of protection for consumer information

BMA
BERMUDA MONETARY AUTHORITY

Cybersecurity and ICPs (cont.)

G7FE 4 - Supervision

- Insurers must have monitoring systems that allow them to ***detect cyber attacks quickly***. Insurers must constantly assess the ***effectiveness of their controls*** in place for cyber risks, including cyber attack simulations

- **ICP 8.1** calls for supervisors to require insurers to establish effective risk management systems, including early warning and risk response systems

- **ICP 8.2** calls for supervisors to require insurers with monitoring systems to run regular effectiveness tests

- Examples of Controls
  - Are there permanent high-risk activity monitoring systems (e.g. access to confidential information)? Is monitoring done in real time?
  - What is being monitored (e.g. at-risk hardware and software)?
  - Is there evidence of simulations run by the insurer?
  - What use has been made of simulation outcomes?

BMA
BERMUDA MONETARY AUTHORITY

Cybersecurity and ICPs (cont.)

G7FEs 5 and 6 – Response and recovery

- Insurers must respond promptly to cyber attacks, aware of the severity of the attack, curtailing its effects, issuing appropriate notifications to whom it may concern, and coordinating and implementing responses that allow them to return to normal operations.

- **ICP 8.1.2** establishes the necessary elements that insurers must take into consideration in order to respond to the materialisation of risks effectively, and in proportion to the materialised risk

- Examples of Controls
  - What policies and procedures are in place at insurers for enhancing awareness of cyber risks (e.g. staff capacity building programmes focused on cyber risks)?
  - **A**re there explicit plans with detailed descriptions of how to respond to attacks?
  - **A**re there explicit plans explaining in detail how to return to normal operations?
  - **A**re there cyber attack notification policies and procedures?
  - What investigations were implemented by the insurer after a cyber attack?

BMA
BERMUDA MONETARY AUTHORITY

Cybersecurity and ICPs (cont.)

G7FEs 7 – Exchange of information

- Insurers must provide information on threats, weaknesses, attacks and responses to attacks in order to improve responses to attacks, limit damages, heighten awareness and promote in-house learning. Insurers must provide information internally and externally, including notifications to government authorities.
- **ICP 8.1.2** particularly the contingency planning topic and **ICP 16.10** (business risk management) provide regulatory support for supervisors requiring insurers to inform them about their cyber risks management systems, as well as risk materialisation.
- **ICP 3, ICP 25 and ICP 26** address the issue of supervisors exchanging information, together with cooperation among supervisors, including cooperation on international crisis management

- Examples of Controls
  - Does the insurer belong to specialised groups exchanging cyber risk information?
  - Does the insurer share cyber risk information with outsourced service providers?

BMA
BERMUDA MONETARY AUTHORITY

Cybersecurity and ICPs (cont.)

G7FEs 8 – Continuous learning

- Insurers must keep their cyber risks management systems constantly under review, in order to ensure that they keep pace with new cyber risks, while also endowing them with adequate resources

- **ICP 16.10** (business risk management) calls for supervisors to require insurers to include a feedback circuit that allows them to take the necessary steps in a timely manner, in response to risk profile changes

- Examples of Controls
  - Are there indications of the existence of feedback circuits in insurer cyber risk management systems? If so, is there evidence that such circuits are functioning effectively (e.g. are they being used)?
  - How often are risk management systems reviewed/updated? How exhaustive are these reviews?

BMA
BERMUDA MONETARY AUTHORITY

Thank you.

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)

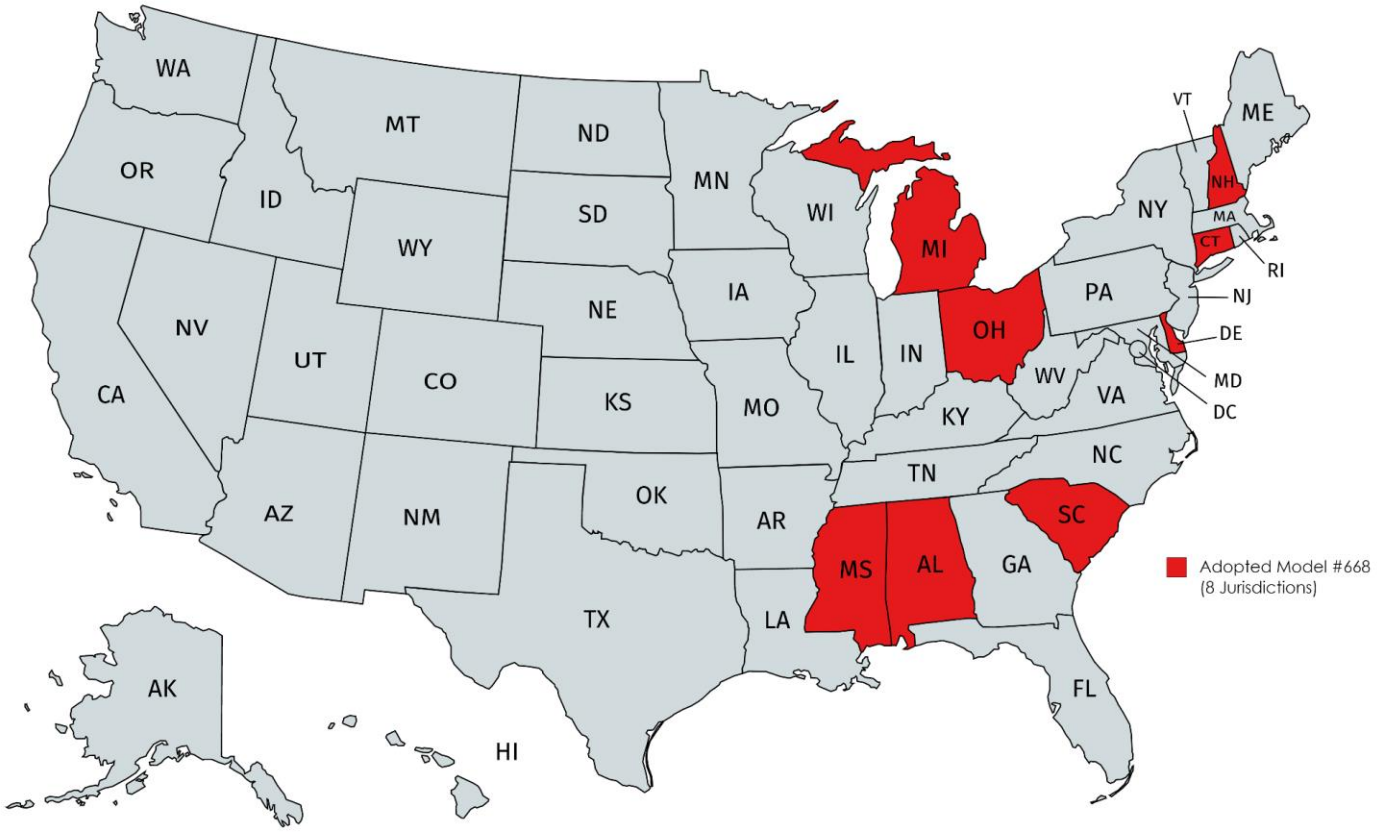
NAIC *Insurance Data Security Model Law* (#668)

Key Provisions	
Section 3: Definitions	
• Cybersecurity Event • Information System • Licensee	• Nonpublic Information (NPI) • Third-Party Service Provider (TPSP)
Section 4: Information Security Program	
• Risk Assessment • Risk Management (Implement Security Measures) • Oversight by Board of Directors • Oversight of TPSPs	• Program Adjustments • Incident Response Plan • Annual Certification
Section 5: Investigation	
• Conduct investigation to determine: ➢ Whether Cybersecurity Event occurred ➢ Assess nature and scope ➢ Identify NPI ➢ Restore system security	• If Event with TPSP, complete investigation or ensure TPSP does so • Maintain records
Section 6: Notification	
• Notify Commissioner within 72 hours • Provide Information about Event	• Notify Consumers (under applicable state law) • Notify TPSP, Reinsurers, Producers, etc.
Section 9: Exceptions	
• Fewer than 10 employees • Certifies compliance with HIPAA	• Employee or agent of a Licensee who is also a Licensee

Comparison: NAIC Model and 23 NYCRR 500

Provision	NY DFS Reg.	NAIC Model
Cybersecurity / Information Security Program	X	X
CISO or other individual/entity responsible for ISP	X	X
Data Retention Policy	X	X
Risk Assessment	X	X
Security Measures / Controls:	Mandated	As Appropriate
• Regular system testing	X	X
• Audit Trails	X	X
• Restrict access privileges	X	X
• Application Security	X	X
• Multi-Factor Authentication	X	X
• Staff Training	X	X
• Encryption of NPI	X	X
Oversight by Board of Directors	X	X
Third-Party Vendor Oversight	X	X
Incident Response Plan	X	X
Annual Certification to Supt. / Commr.	X	X
Notify Supt. / Commr. (72 hrs.)	X	X
Exceptions for smaller entities	X	X

Implementation of Model Act #668
Insurance Data Security Model Law
[status as of August 6, 2019]



This map represents state action or pending state action addressing the topic of the model. This map does not reflect a determination as to whether the pending or enacted legislation contains all elements of the model or whether a state meets any applicable accreditation standards.

NAIC Financial Examinations

- IT Review is part of Financial Exam
  - Guidance initially based on COBIT Framework
  - Addresses IT general controls including key security concepts
  - Consistent with rest of the broader financial exam, IT Review is risk-focused

- Cybersecurity updates to the NAIC *Financial Condition Examiners Handbook* (annually since 2015)
  - Updates based on NIST Framework (Identify, Protect, Detect, Respond and Recover)
  - Added or enhanced language on concepts such as:
    - Network monitoring
    - Vulnerability and patch management
    - Third-party network access

- Cybersecurity checklists adopted as part of the *Market Regulation Handbook*
  - Pre-breach and post-breach checklists
  - Based on the Insurance Data Security Model Law (#668)

Thank You.

Save the Date! Next Consultation Call on

21 November, 2019

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)