



# Cyber Risk in the Insurance Sector

A2ii – IAIS Consultation Call

26 September 2019

## Expert



**Andrea Camargo**  
Director “Inspowering”,  
Technical Expert, A2ii

## Supervisory Presenter



**Glory Kasasi**  
Principal ICT Examiner, Pension  
and Insurance Supervision, Reserve  
Bank of Malawi

## 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



# Topics to be Addressed

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

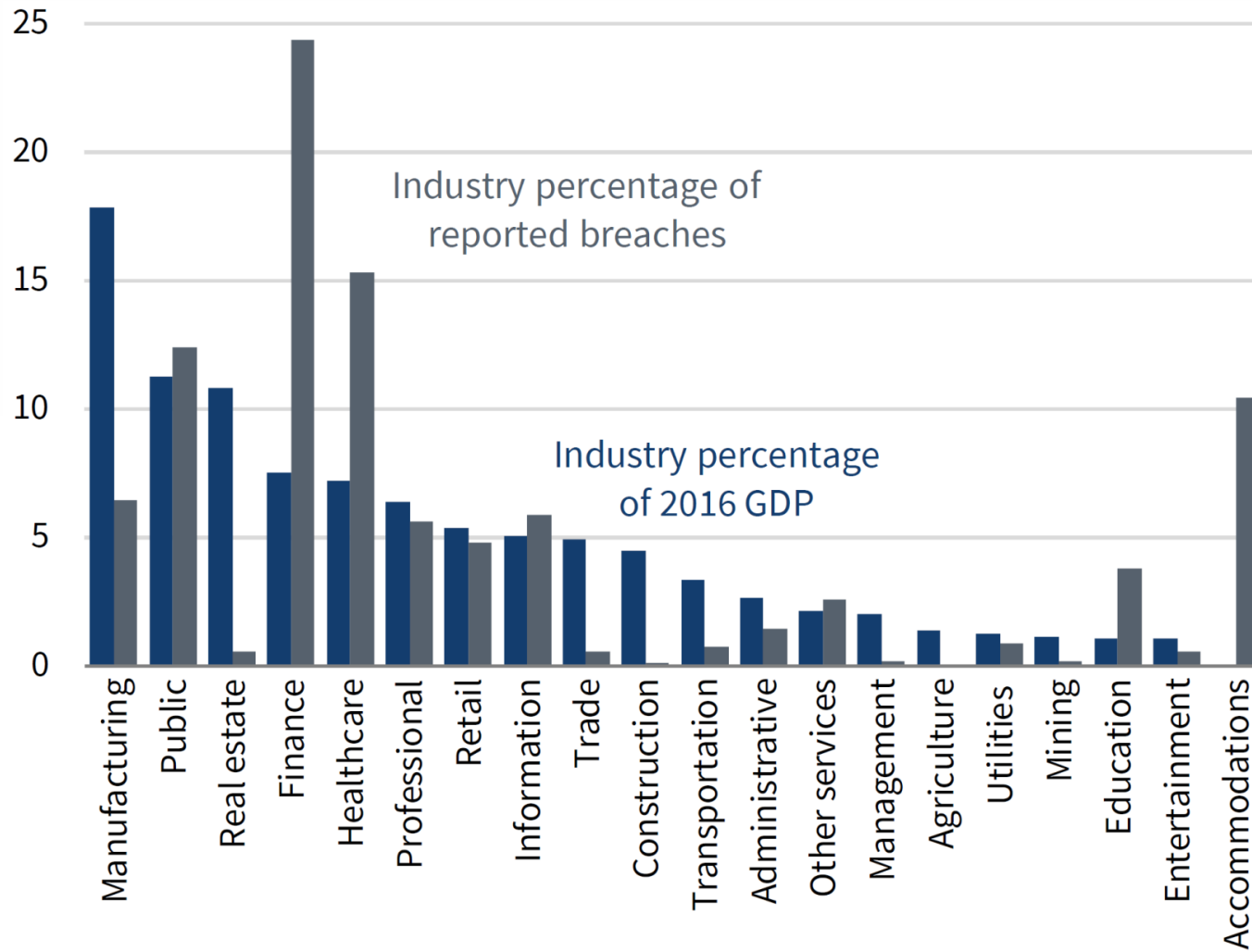


# Cyber Attacks and Cyber Risks

- **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.

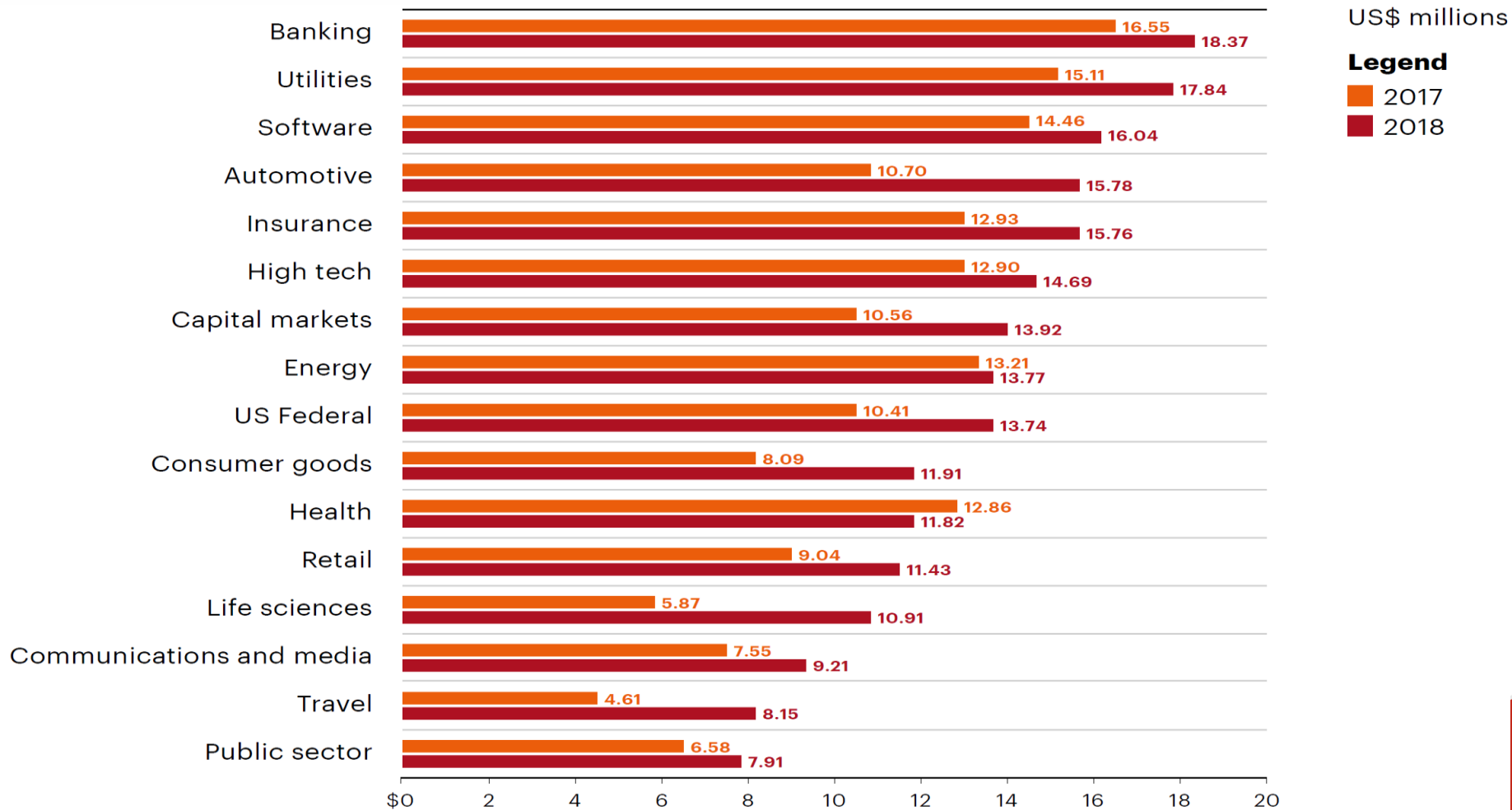
# Cyber Attacks and the Financial Sector



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

# Cyber Attacks – Economic Damage

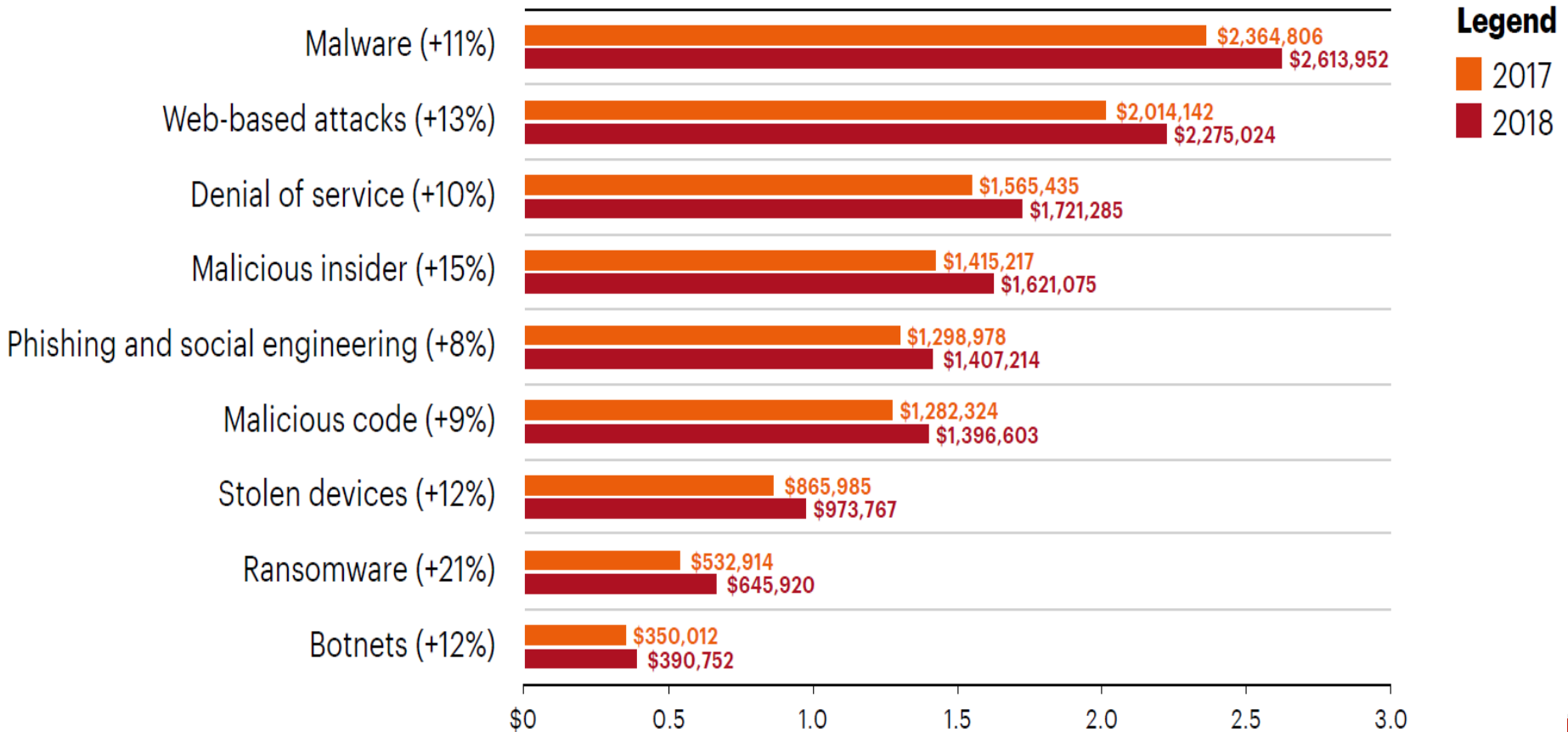
## Mean Annual Costs of Cyber Attacks by Sector



Source: Accenture (2019) The cost of cyber crime

# Cyber Attacks – Economic Damage

## Mean Annual Costs of Cyber Attacks by Type of Attack

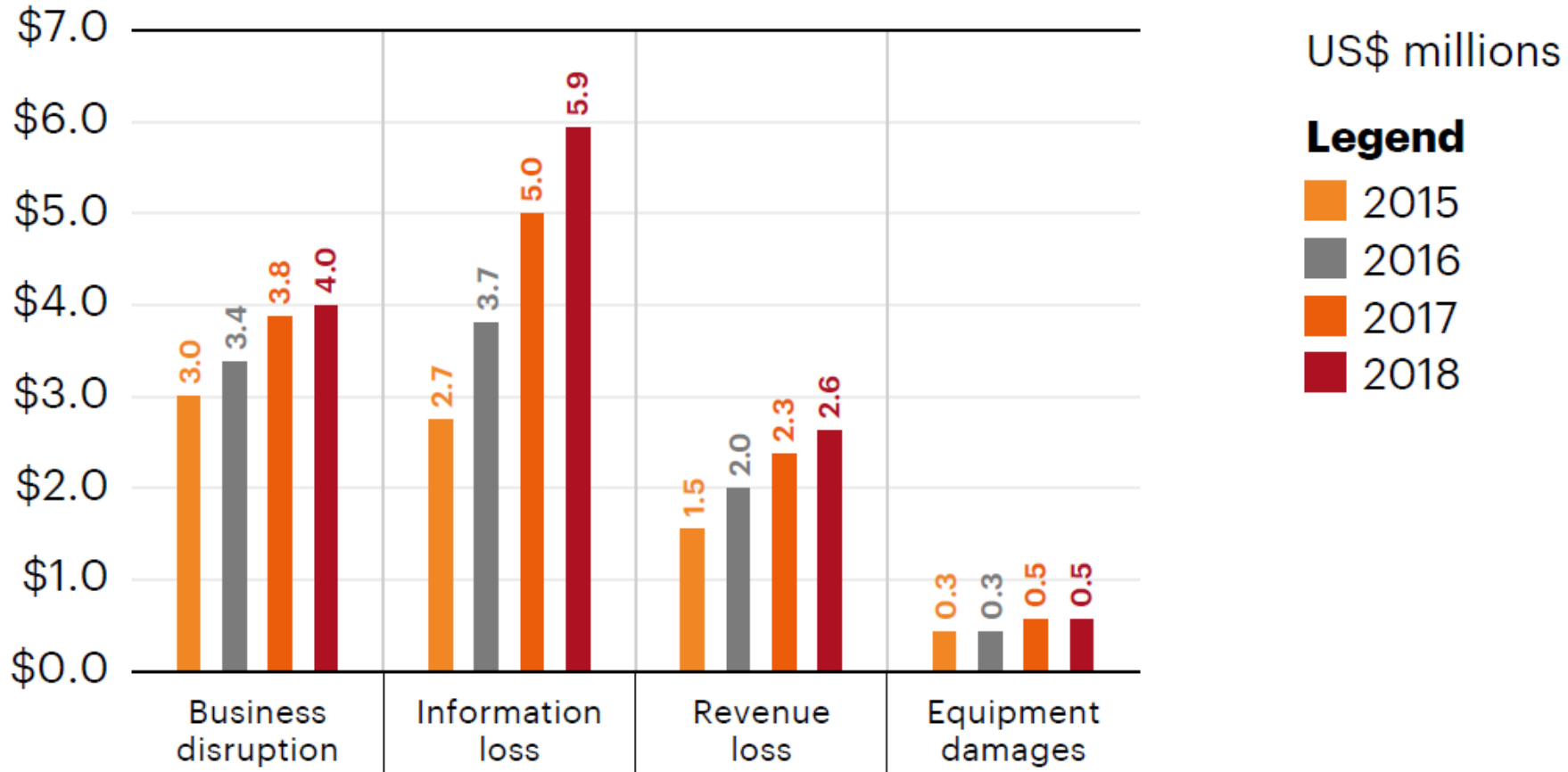


**Source:** Accenture (2019) The cost of cyber crime



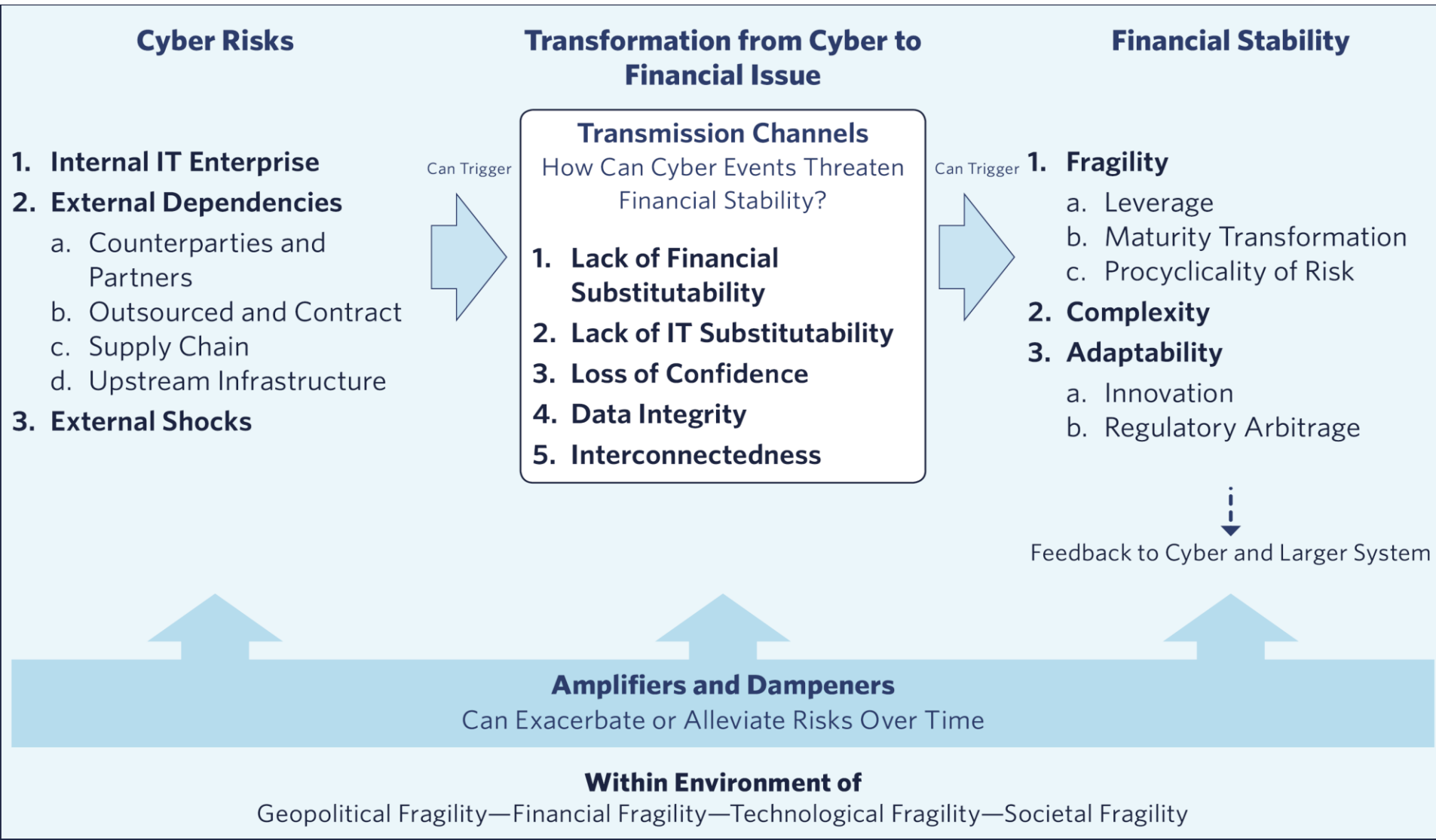
# Cyber Attacks – Economic Damage

## Mean Annual Costs of Cyber Attacks by Consequences of the Attack



Source: Accenture (2019) The cost of cyber crime

# Cyber Attacks and Financial Stability



# Topics to be Addressed

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



# 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

# 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.

# 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

# 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?

# 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?



# 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

# 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?

# 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)?
  - Are there explicit plans with detailed descriptions of how to respond to attacks?
  - Are there explicit plans explaining in detail how to return to normal operations?
  - Are there cyber attack notification policies and procedures?
  - What investigations were implemented by the insurer after a cyber attack?

# 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?

# 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?

Thank you.

Follow us on Twitter [@a2ii\\_org](#), Youtube and LinkedIn

# AN OVERVIEW OF SUPERVISION OF INFORMATION AND CYBER SECURITY RISK: CASE OF MALAWI

Presented By  
**Glory Kasasi**

*Principal Examiner, ICT - Pension and Insurance Supervision Department  
Reserve Bank of Malawi*





# OUTLINE

- Background
- Cyber regulation in Malawi
- ICT Supervision
- Weaknesses and challenges
- Current work





# BACKGROUND

- Reserve Bank of Malawi (RBM) is the sole regulator of the financial sector in Malawi.
- Supervision of the financial sector is carried out under the following departments within RBM;
  - Financial Sector Regulation – Policy and regulation formulation and enforcement
  - Bank Supervision- Banks and Credit Reference Bureaus
  - Pension and Insurance supervision
  - Capital Markets and Microfinance Supervision
- RBM largely applies Risk Based Supervision approach



# BACKGROUND

- At first ICT exams were only done for banks; exams for insurance companies started around 2011
- An IT landscape survey was conducted among insurance companies about 5 years ago which showed significant use of ICT amongst the insurers including use of mobile services, customer online portals
- the increasing dependence of financial institutions on technology has necessitated ICT risk to be examined separately
- ICT examinations are normally conducted as part of the normal prudential examination routines but separated from operational risk to adequately examine the IT environment
- Include international best practice as well in relation to ICT oversight
- Combined or separate coverage and reporting of IT risks depending on the size of the company i.e. sometimes covered under operational risk



# BACKGROUND

## ICT Examination Areas

1. IT Governance
2. IT Risk Management framework
3. Management of outsourcing risks
4. Acquisition and development of Information Systems
5. IT service management
6. Systems reliability, availability and recoverability
7. Management of Operational infrastructure security
8. Data Centre protection and controls
9. Access control



# CYBER REGULATION IN MALAWI

- At National level there is a Cyber Security Act of 2016 and a National Cyber Security strategy (2018)
- Due to advanced technologies in the financial industry, there are risks and threats that have emerged in the cyber space that require adequate supervision to ensure that IT environment of the supervised entities is protected.
- RBM issued Risk management directive for insurers
- IT risk management guidelines available for banks and separate guidelines for pension administrators:
  - To strengthen IT governance
  - To establish sound and robust technology risk management
  - To strengthen system security, reliability, resilience and recoverability
- As for insurers, IT risk covered in the draft risk management guidelines for insurers but not comprehensively



# ICT SUPERVISORY TOOLS

- Questionnaire containing questions on expected controls used for offsite and onsite supervision
- Pre-examination requests
- Draft IT questionnaire for IT and risk officers under pilot
- Commonwealth insurance supervision manual
- FDIC onsite tools (adapted)



# WEAKNESSES & CHALLENGES

- Lack of understanding by some of the insurers on cyber risk
- Currently no overview of cyber threat landscape for the insurance sector
- Cyber response structure is missing
- Absence of formal guidance as to how incidents in regulated institutions should be communicated to other potentially effected divisions within RBM or other relevant authorities in Malawi



# CURRENT & FUTURE DEVELOPMENTS

- IMF bilateral Technical Assistance (TA) mission on Information and Cyber Security Risk Supervision is underway
- Currently updating the IT risk management guidelines for banks to incorporate cyber risk issues
- Final product will be Cyber Security Risk Management guidelines applicable to all relevant supervised financial institutions to be issued in 2020
- To formalizing cyber crisis management plans and conducting crisis exercises
- Establish a cyber incident reporting mechanism for supervised institutions

**THE END  
THANK YOU.**



Thank You!  
Save the Date! Next Consultation Call on **21  
November, 2019**

Follow us on Twitter @a2ii\_org, Youtube and LinkedIn