EIOPA Cyber Insurance Workshop
1st April 2019

How to improve understanding of cyber risks and align with clients needs?

Philippe Cotelle

Board member of FERMA and Head of Risk and Insurance Management, AIRBUS DS

Four questions to answer today

1. What is needed to enhance understanding?
2. What is the role of underwriters and brokers?
3. What are the obstacles preventing a better understanding?
4. What is the role of the supervisors and/or regulators?

Our joint cyber insurance project

First-time collaboration w/ the Insurers and Brokers Federations in Brussels, to help midcaps to **prepare the underwriting information** and **compare the cyber insurance offers**

First presentation of « *Preparing for Cyber Insurance* » **at the FERMA Seminar 2018**

Preparing for cyber insurance

Available on FERMA website

bipar

FERMA
Federation of European Risk Management Associations

insurance europe

with the contribution of

AON Empower Results*

MARSH

October 2018

Preparing for Cyber Insurance

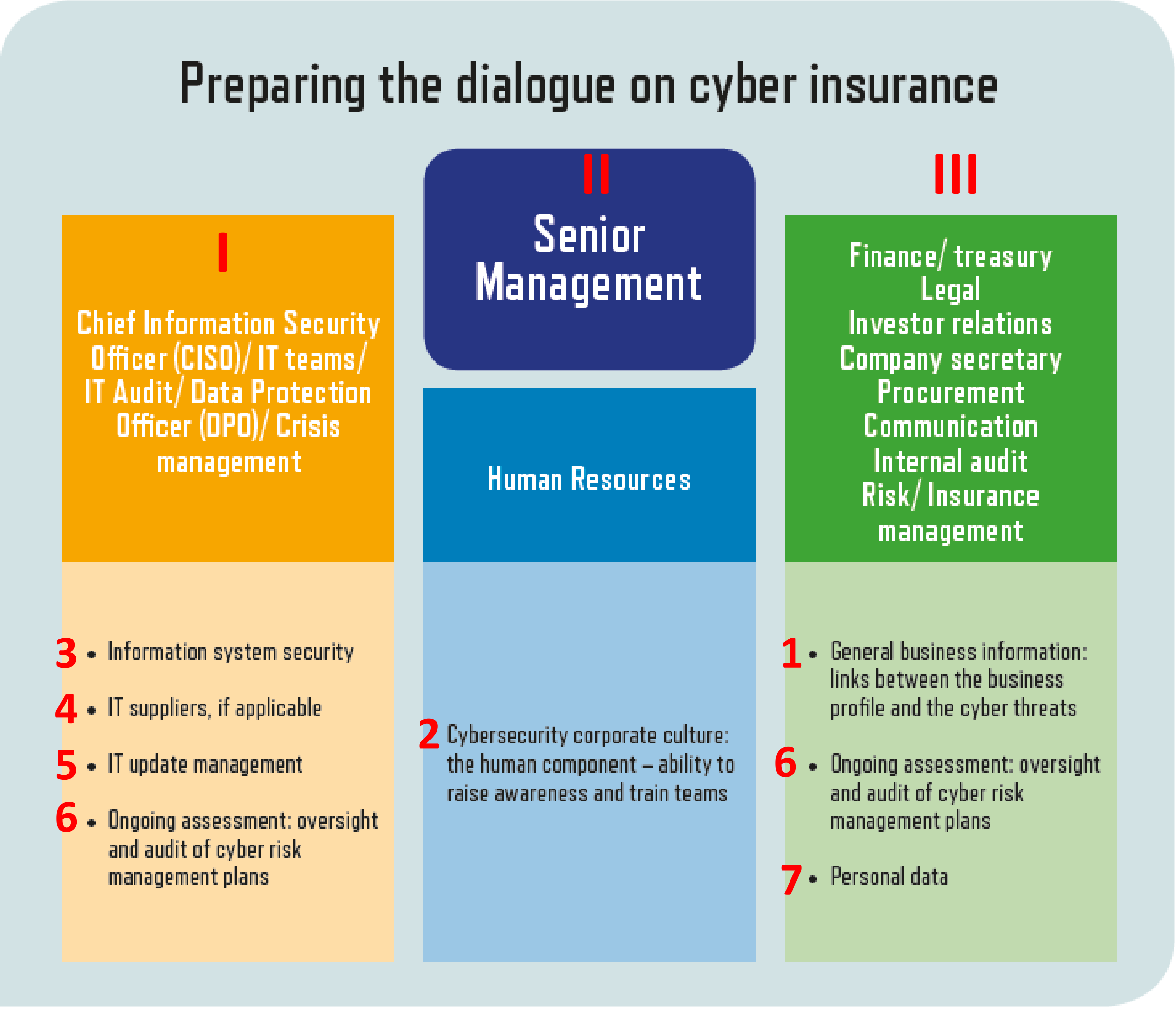
WHAT IS NEEDED TO ENHANCE UNDERSTANDING?

Prepare for the dialogue on cyber insurance

Underwriting info to prepare internally - 7 blocks of information

Where to find the underwriting info?

3 blocks: IT area (I), Human resources (II), Corporate functions (III)



Preparing the dialogue on cyber insurance

I

Chief Information Security Officer (CISO)/ IT teams/ IT Audit/ Data Protection Officer (DPO)/ Crisis management

- 3 Information system security
- 4 IT suppliers, if applicable
- 5 IT update management
- 6 Ongoing assessment: oversight and audit of cyber risk management plans

II

Senior Management

Human Resources

2 Cybersecurity corporate culture: the human component – ability to raise awareness and train teams

III

Finance/ treasury
Legal
Investor relations
Company secretary
Procurement
Communication
Internal audit
Risk/ Insurance management

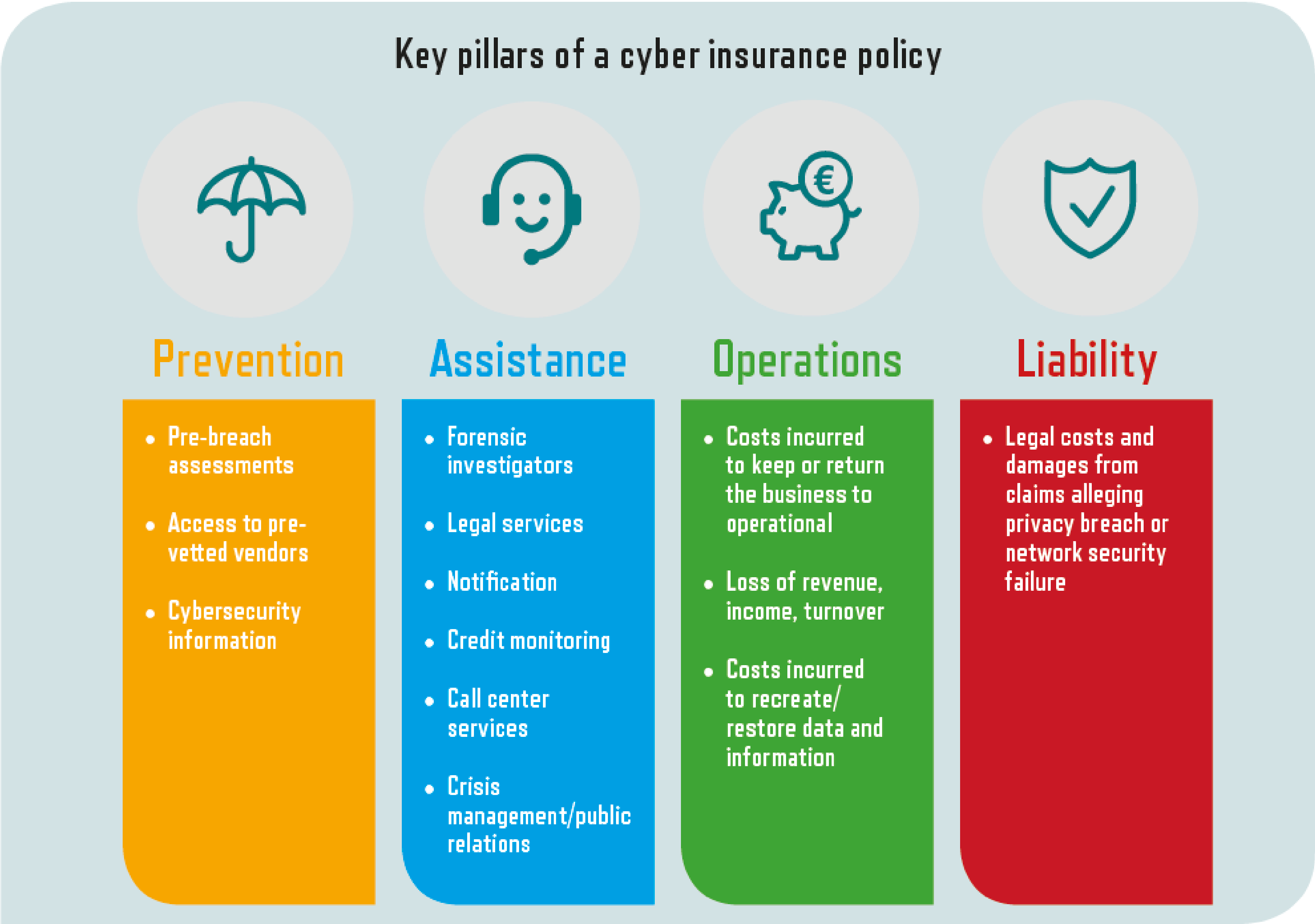
- 1 General business information: links between the business profile and the cyber threats
- 6 Ongoing assessment: oversight and audit of cyber risk management plans
- 7 Personal data

Preparing for Cyber Insurance

WHAT IS THE ROLE OF UNDERWRITERS AND BROKERS?

Improve comparability of cyber insurance offers

Objective for the reader: better **understand the various cyber insurance offers** and the different degrees of cover and service levels



Key pillars of a cyber insurance policy

Prevention

- Pre-breach assessments
- Access to pre-vetted vendors
- Cybersecurity information

Assistance

- Forensic investigators
- Legal services
- Notification
- Credit monitoring
- Call center services
- Crisis management/public relations

Operations

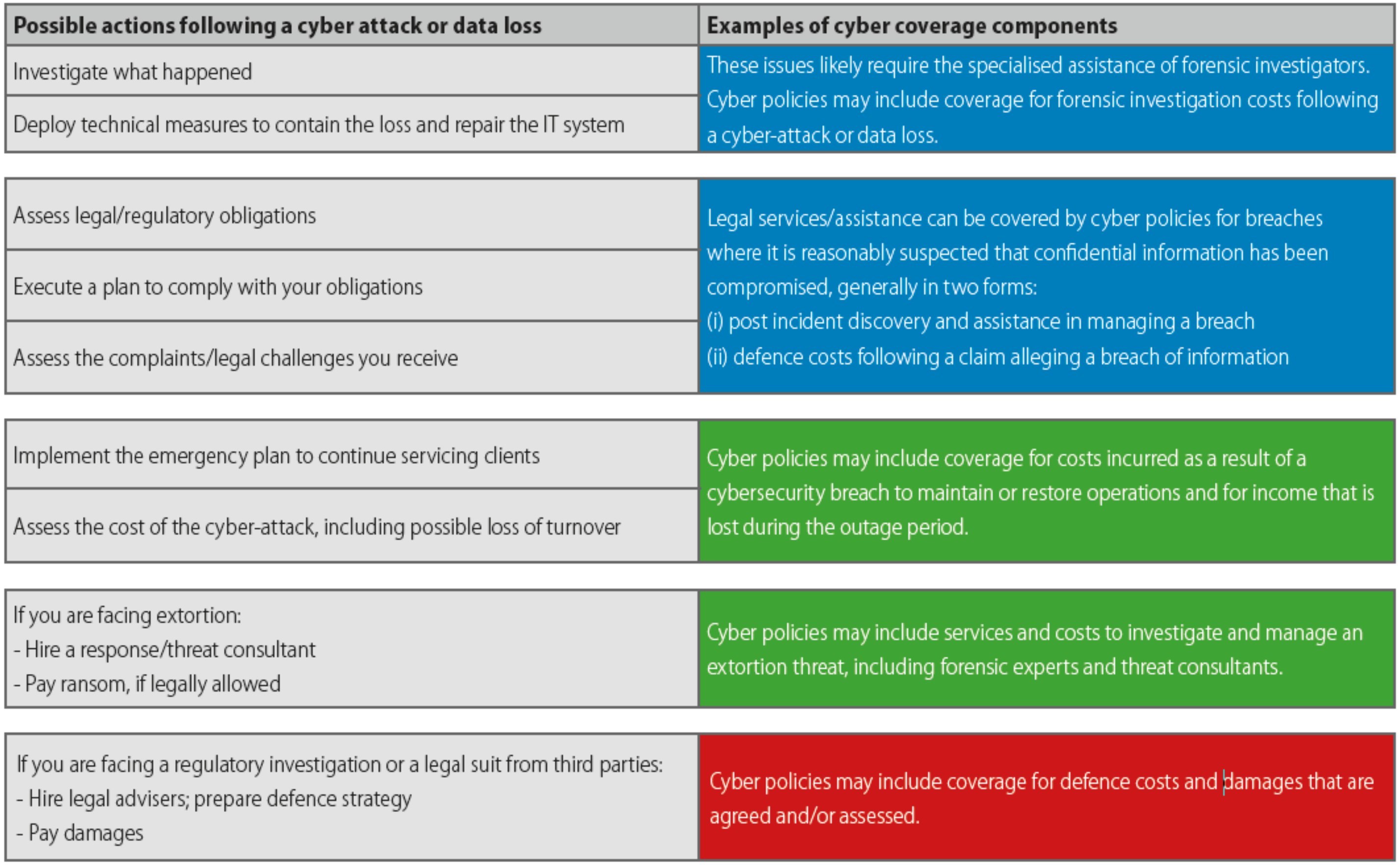
- Costs incurred to keep or return the business to operational
- Loss of revenue, income, turnover
- Costs incurred to recreate/ restore data and information

Liability

- Legal costs and damages from claims alleging privacy breach or network security failure

3 tools to improve comparability

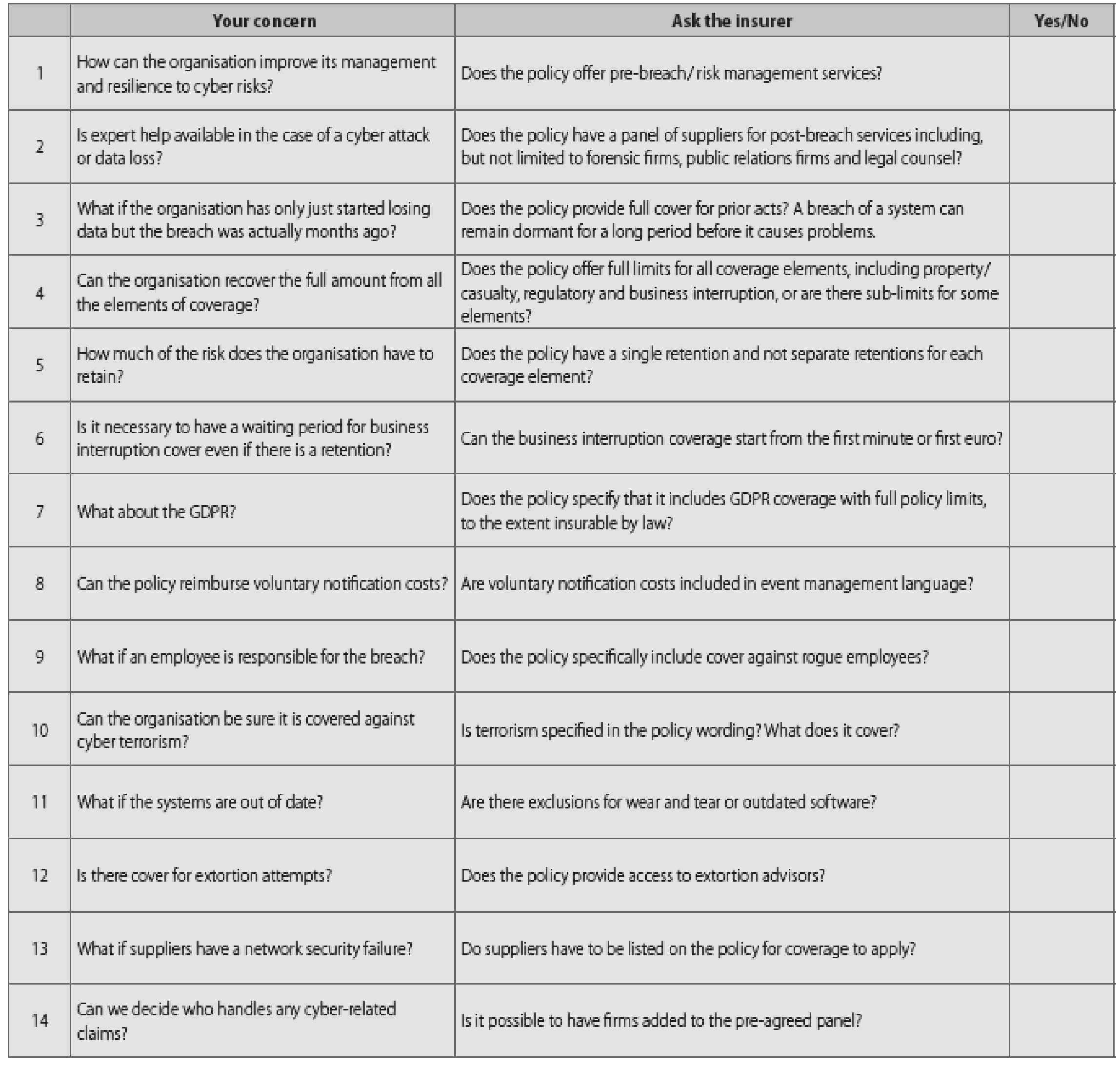
Tool 1: Cyber coverage components — It shows how cyber insurance policies may be able to respond at the various stages of a cyber event



Possible actions following a cyber attack or data loss	Examples of cyber coverage components
Investigate what happened	These issues likely require the specialised assistance of forensic investigators. Cyber policies may include coverage for forensic investigation costs following a cyber-attack or data loss.
Deploy technical measures to contain the loss and repair the IT system	
Assess legal/regulatory obligations	Legal services/assistance can be covered by cyber policies for breaches where it is reasonably suspected that confidential information has been compromised, generally in two forms: (i) post incident discovery and assistance in managing a breach (ii) defence costs following a claim alleging a breach of information
Execute a plan to comply with your obligations	
Assess the complaints/legal challenges you receive	
Implement the emergency plan to continue servicing clients	Cyber policies may include coverage for costs incurred as a result of a cybersecurity breach to maintain or restore operations and for income that is lost during the outage period.
Assess the cost of the cyber-attack, including possible loss of turnover	
If you are facing extortion: - Hire a response/threat consultant - Pay ransom, if legally allowed	Cyber policies may include services and costs to investigate and manage an extortion threat, including forensic experts and threat consultants.
If you are facing a regulatory investigation or a legal suit from third parties: - Hire legal advisers; prepare defence strategy - Pay damages	Cyber policies may include coverage for defence costs and damages that are agreed and/or assessed.

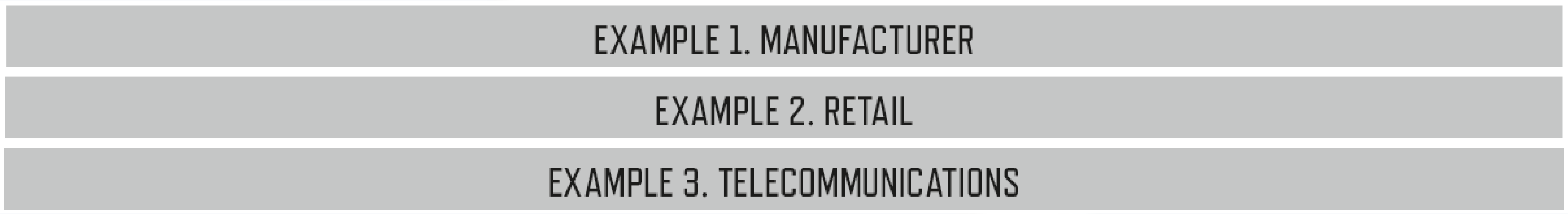
3 tools to improve comparability

Tool 2: Coverage checklist— 14 sample questions to ask to the insurer based on typical business concerns on cyber



	Your concern	Ask the insurer	Yes/No
1	How can the organisation improve its management and resilience to cyber risks?	Does the policy offer pre-breach/ risk management services?	
2	Is expert help available in the case of a cyber attack or data loss?	Does the policy have a panel of suppliers for post-breach services including, but not limited to forensic firms, public relations firms and legal counsel?	
3	What if the organisation has only just started losing data but the breach was actually months ago?	Does the policy provide full cover for prior acts? A breach of a system can remain dormant for a long period before it causes problems.	
4	Can the organisation recover the full amount from all the elements of coverage?	Does the policy offer full limits for all coverage elements, including property/ casualty, regulatory and business interruption, or are there sub-limits for some elements?	
5	How much of the risk does the organisation have to retain?	Does the policy have a single retention and not separate retentions for each coverage element?	
6	Is it necessary to have a waiting period for business interruption cover even if there is a retention?	Can the business interruption coverage start from the first minute or first euro?	
7	What about the GDPR?	Does the policy specify that it includes GDPR coverage with full policy limits, to the extent insurable by law?	
8	Can the policy reimburse voluntary notification costs?	Are voluntary notification costs included in event management language?	
9	What if an employee is responsible for the breach?	Does the policy specifically include cover against rogue employees?	
10	Can the organisation be sure it is covered against cyber terrorism?	Is terrorism specified in the policy wording? What does it cover?	
11	What if the systems are out of date?	Are there exclusions for wear and tear or outdated software?	
12	Is there cover for extortion attempts?	Does the policy provide access to extortion advisors?	
13	What if suppliers have a network security failure?	Do suppliers have to be listed on the policy for coverage to apply?	
14	Can we decide who handles any cyber-related claims?	Is it possible to have firms added to the pre-agreed panel?	

3 tools to improve comparability



EXAMPLE 1. MANUFACTURER

EXAMPLE 2. RETAIL

EXAMPLE 3. TELECOMMUNICATIONS

Tool 3: Scenarios — involving fictional large mid-mkt organisations and showing possible insurance coverages with:

- Interplay between cyber insurance policies and other lines of insurance
- Coverage considerations of this scenario in the various cyber insurance offers

Preparing for Cyber Insurance

WHAT ARE THE OBSTACLES PREVENTING A BETTER UNDERSTANDING?

Clarity and certainty for the insureds

- **Reduce legal and contractual uncertainty**
- **Increase trust and confidence in claims settlement**
  - Conditions for claim settlement are very specific for cyber risks
    - Need to clarify the procedure where the client is asked to demonstrate:
      - The occurrence of a technical trigger giving rise to an insurance claim
      - The occurrence of insurable impacts as consequences of this trigger
    - Need for success stories as the best promotion for cyber insurance - demonstration of a successful claim management

Preparing for Cyber Insurance

WHAT ROLE FOR REGULATORS AND SUPERVISORS?

Roles of regulators and supervisors

- **To be discussed:**
  - *Take into account the needs and perspective of corporate clients*
  - *Set up neutral platform to support citizens and businesses and centralize cyber incident information*
  - *Role in state-sponsored attack, problem of attribution and consequences on contracts (war exclusion)*
  - *Not relevant to impose standards and norms*

FERMA

Many thanks for your attention!

Preparing for cyber insurance

Available on FERMA.eu website

bipar

FERMA

Federation of European Risk Management Associations

insurance europe

with the contribution of

AON Empower Results

MARSH

October 2018