05.

CUSTOMERS' PERSPECTIVE ON CYBER INSURANCE

dr. Marie Gemma Dequae

Insurance and Reinsurance Stakeholder Group meeting

7 February 2018

AGENDA

1. Conditions before opening a dialogue with the insurance market
2. Necessity to improve cyber insurance market practices

1 - Conditions before opening a dialogue with the insurance market

A. the organisation must **understand its exposure** to cyber risks (through a proper cyber risk governance)

B. once cyber risk exposure is defined, the organisation **decides which investments** are needed to increase cyber protection level based

C. the organisation should determine which cyber risks may **already be insured** under existing insurance policies to determine the residual risk

Understand the cyber exposure

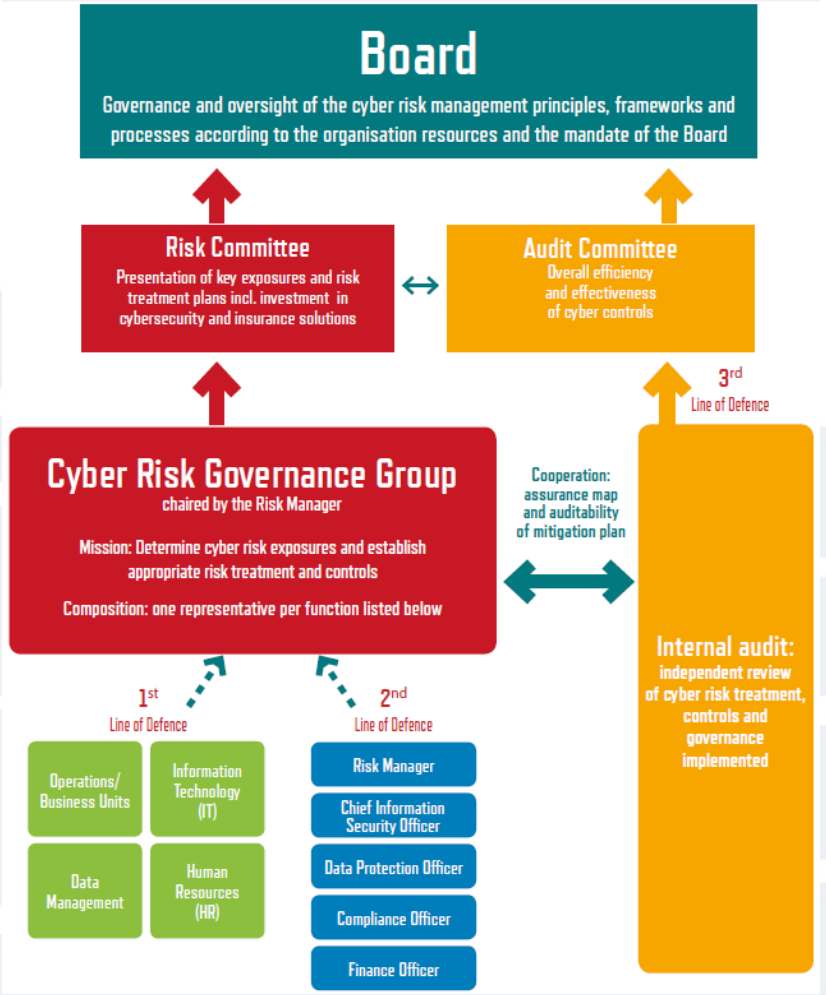
A business need	• Help organisations to **increase their resilience** to cyber events* while **creating value with digitalization opportunities**
New cyber laws*	• introducing **new IT security and legal requirements** for organisations but remain silent on the governance aspect of cybersecurity
Beyond IT, a corporate issue	• **Risk management readiness** can only be achieved within a strong governance framework, and through a **highly coordinated approach across all departments of an organization**

FERMA proposal to assess cyber exposure

THE CYBER RISK GOVERNANCE GROUP

- **A cross-function team headed by the risk manager**
  - Composed of operational functions from the 1st line of defence and key functions from the 2nd line of defence*
  - To **determine cyber risk exposures** in financial terms and **design possible mitigation plans**

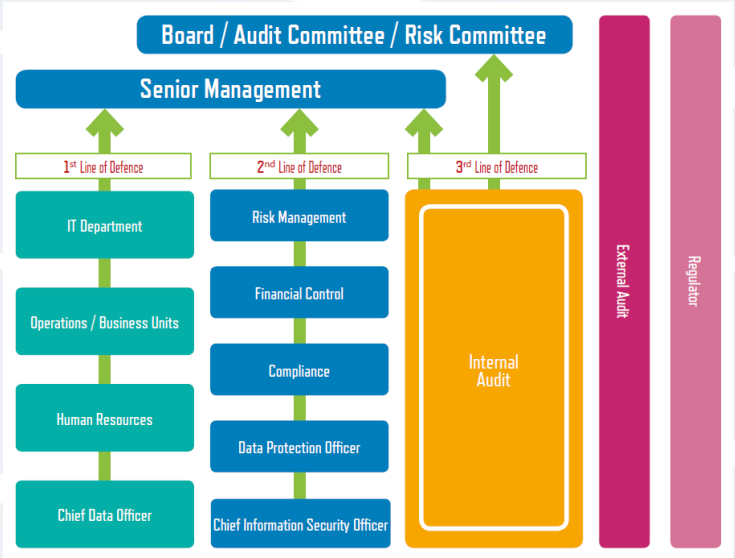
- **Why cross-disciplinary?**
  - Expertise, by being cross-disciplinary, the group has the **subject and organisational knowledge** to identify the most harmful cyber risks for the organisation and list the suitable responses



Two strong pillars to support the proposal

- The eight principles set out in the **OECD recommendation on Digital Security Risk Management** (2015)

- The **Three Lines of Defence model**, recognised as a standard of Enterprise Risk Management (ERM)



2- Necessity to improve cyber insurance market practices

A. Taking into account the needs of the insured's
B. Providing recommendations for cyber insurance best practices

A. Taking into account the needs of the insured's

- First step should start from the situation faced by the client before any decision to purchase cyber insurance
- What are the clients needs and what are they ready to buy? For which residual risk?
- Gap between the demand and the offer which do not meet is one of the major obstacles to the development of the market.
- Seek to reach a consensus between the client (the demand) and the market (the offer)

A. Taking into account the needs of the insured's

- Risk assessment should not only start from the insurer side but from the customer side
- The client needs to define the exposition faced by his organization to cyber risk from his business perspective.
- The Risk assessment language should be defined at the intersection of clients, brokers and insurance languages.

A. Taking into account the needs of the insured's

- Brokers and insurers are unable to quantify the financial exposure of the client
- The cyber risk identification and quantification from the perspective of the client is not enough taken into account
- The market, including risk and insurance managers, is in need for cyber risk financial quantification

A. Taking into account the needs of the insured's

- There is no "typical" exclusion of cyber risks from traditional commercial general liability policies
- Many cyber risk consequences are covered in traditional contract: the challenge is *cyber silent covers.*

B. Providing recommendations for cyber insurance best practices

Three areas of improvement

1. The exchange of information between insurers and insureds – Clarify underwriting information
2. Clarity for the insureds the key components of cyber insurance contract
3. Clarification over cyber claims management

B1 - Information exchanged between insurers and insureds

What level of information is requested by the insurers?

One goal: achieve a greater standardisation in the information provided in *underwriting/ subscription quotes/ offers* (offres de souscription).

B2 - Clarity for the insureds the key components of cyber insurance contract

- Facilitate comparison of cyber insurance quotes: stand alone offer or add-on in existing insurance policies
- Minimum elements of information to be provided in a standardised way on the coverage, limits, exclusions
- Connection between cybersecurity products in general and cybersecurity standard
- Need to be updated very regularly

B3 - Clarification over cyber claims management

- A client will buy an insurance coverage when he knows when and how he can activate his contract and get claim upon his contract
  - Includes financial compensation but also a full range of services,
  - Confidentiality claim assessment, forensic expertise evidence, etc.

CONCLUSION

- After having put in place a strong cyber risk governance,
- the next steps for the corporate insurance buyers will be to define:
  - A better exchange of information with the insurers
  - An easier way to compare the cyber insurance offerings
  - Clear cyber claims management procedures