



CYBER RISKS

FROM AN INSURANCE PERSPECTIVE

**Workshop on Expert Judgement for Geographical and Adversial Problems
April 15 - 17, 2015**

**Kristof Vanooteghem
Chief Technical Officer Commercial Lines
AXA Spain**

Overview

- ➔ Definition
- ➔ Risk
- ➔ Risk consciousness
- ➔ Risk management
- ➔ Insurance
 - ➔ Role
 - ➔ Current situation
 - ➔ Near future
- ➔ Conclusions

Definition: Cyber risk is inherent to the use of IT systems

'Cyber risk' means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems. (IRM, Institute for Risk management)

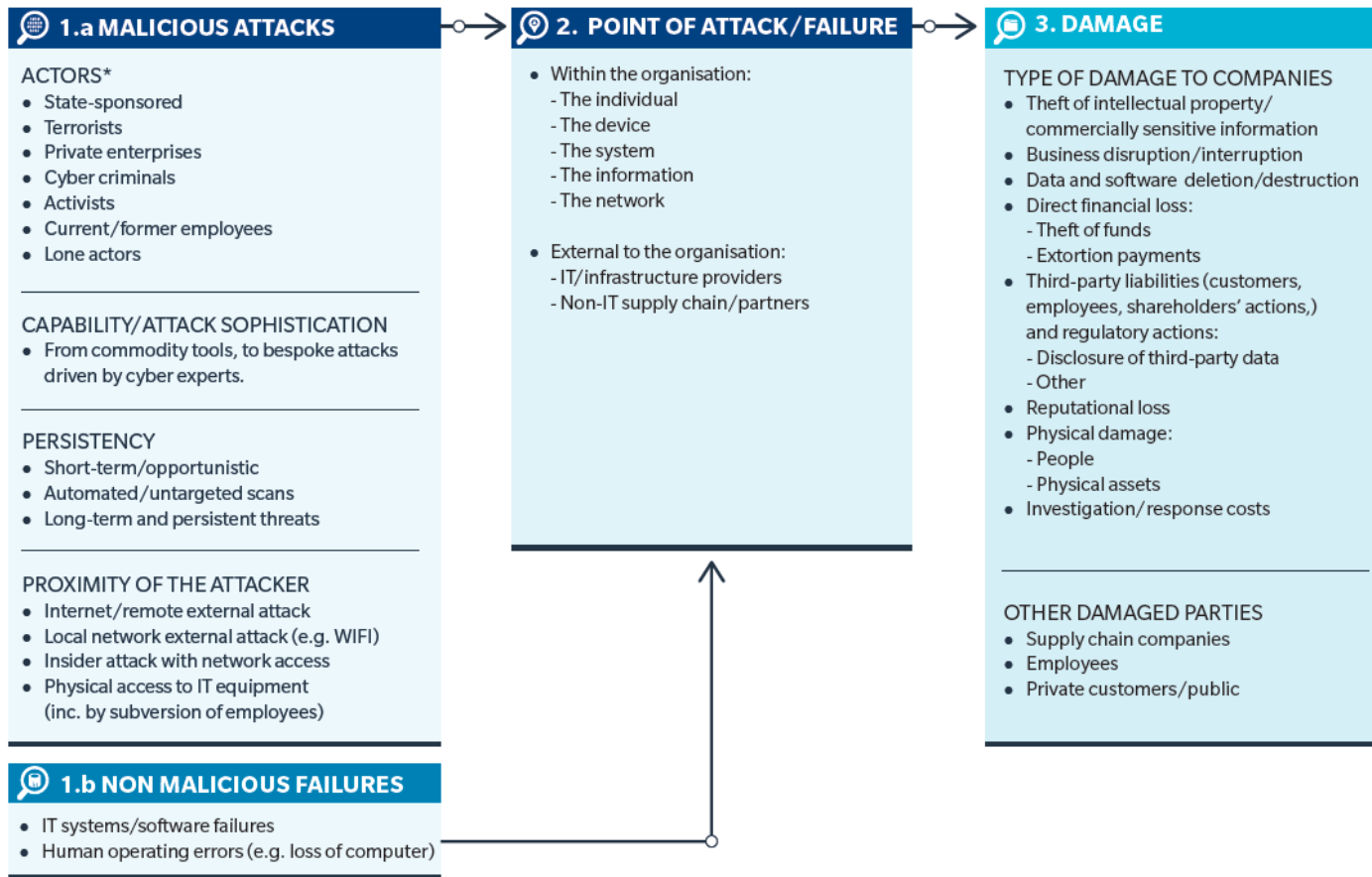
However in its broadest form cyber risk can be a synonym for IT risk, i.e. "The business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise" (ISACA IT Risk framework)



Common mistakes in our industry:

- 'Cyber risk' is not limited to data protection, but is the most common aspect and most insured due to specific data breach regulation
- Not limited to malicious acts: over 60% of data breaches are non malicious

Risk profile of Cyber risks



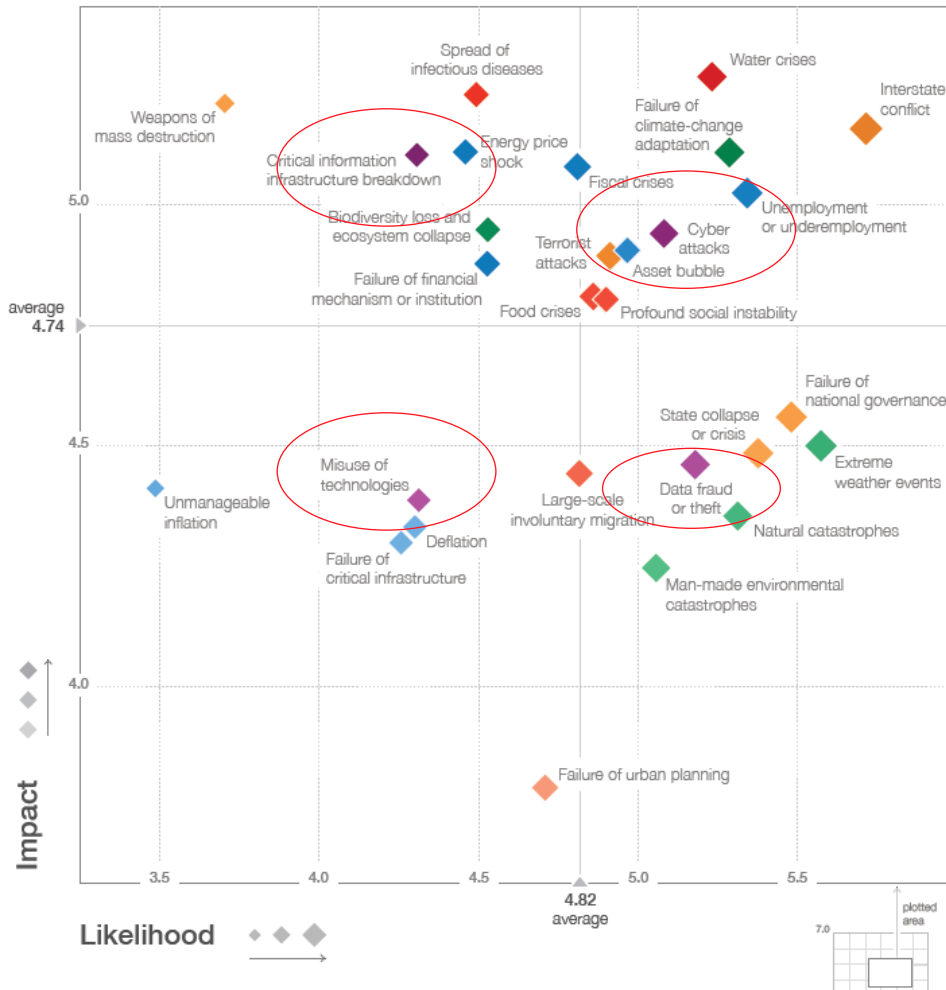
* Actors often correlated with MOTIVATION (1 Warfare/terrorism, 2 Propaganda, 3 Commercial gain/advantage, 4 Direct financial gain, 5 Protest, 6 Fun/demonstrate ability, 7 Revenge).

UK Cyber security Study, March 2015

Risk consciousness is increasing...

World Economic Forum 2015: Cyber risks amongst Top 10 in terms of likelihood and Impact

Figure 1: The Global Risks Landscape 2015



Allianz Risk Barometer 2015 Cyber crime (!...) with a 5% raise

Risk Barometer Risers and Fallers



The Risers and Fallers chart shows the changes in overall risk perception in the Risk Barometer year-on-year. Concerns over political/social upheaval, war have seen the biggest increase, climbing nine positions to 9th in 2015, up 7%. Conversely, businesses are much less worried about market stagnation this year, which drops two positions to 7th, down 4%. Companies are much worried about the impact of technological innovation (see page 14) long-term than they are short-term.

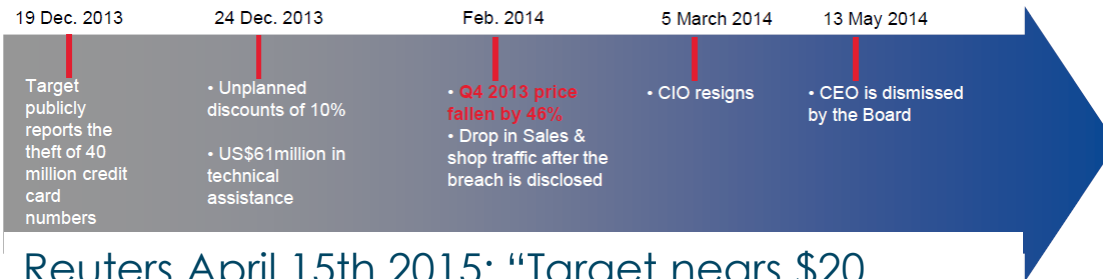
Source: Allianz Risk Barometer 2015, Allianz Global Corporate & Specialty

... and there are good reasons for it

- ➔ Aramco case: Saudi Arabian Oil Company - **Virus** « Shamoon », specifically customized
 - Only mean of communications during 15 days = a fax
 - 30 000 computers infected and destroyed
 - Websites inaccessible Direct costs (PC replacement only)
 - TOTAL \$ 20million
 - > Operational and Business impact



- ➔ Target case: large US retail company – **Data Breach**




Reuters April 15th 2015: "Target nears \$20 million MasterCard data breach settlement: WSJ"



Target Corp. Share price
Dec. 2013 – Feb. 2014

... and there are good reasons for it

- ➔ In February 2015, Anthem suffered a **data breach** of nearly 80 million records, including personal information such as names, social security numbers, dates of birth, and other sensitive details.
- ➔ Specific pain point: **health & personal data**, higher “criminal “ value than credit card data allowing to “take over your life”
- ➔ According to data from the UK dept. for Business Innovation and Skills, 81 % of large businesses and 60% of small businesses suffered a cyber security breach in 2014 with increasing average costs.
- ➔ Average cost in 2013: \$136 per record (up to \$199 in Germany) 2013 PONEMON COST OF DATA BREACH STUDY)
- ➔ Global UK PML estimated at £20 billion -> Accumulation risk!

“But we are already protected”

¿Are we?

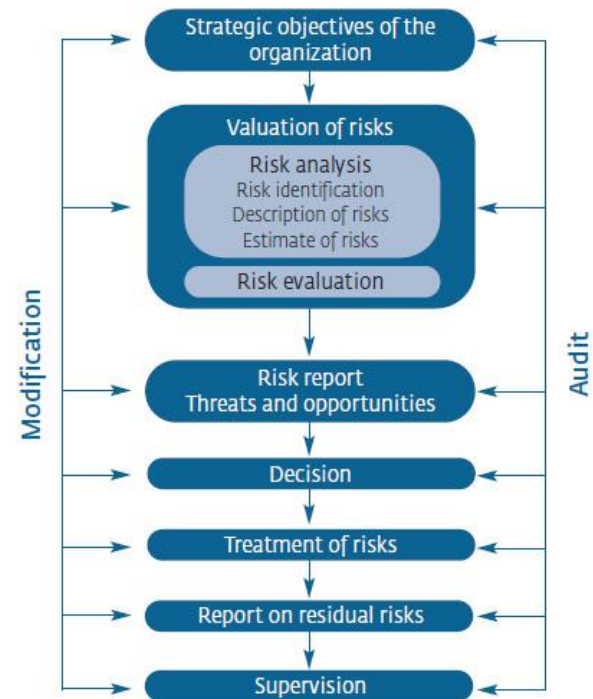
	SOURCE	VALUE
Percentage of CEOs or CIOs of large organisations who believe they have insurance that would cover them in the event of a breach.	BIS, Information Security Breaches Survey 2014	52%
Percentage of CROs or CFOs who state that their organisation has bought cyber insurance.	Marsh and Zurich cyber risk surveys	15%-20%
Percentage of firms with cyber cover, whether as stand-alone cover or implicit in other policies.	Marsh and Zurich cyber risk surveys	10%
Actual penetration of standalone cyber insurance products among UK large businesses.	Estimate based on policies placed/written by project participant	2%

Half of the Large Companies in the UK believe they are adequately protected, while this is more than doubtful:

Source: UK Cyber Security report

This is a result of inadequate risk management: the risk is there, the global awareness is there but the local application is missing:

- ➔ Lack of risk assessment
 - More and more tools available:
 - Cyber Essentials scheme in the UK, Willis Prism –Re™ Feb '15), Aon Cyber diagnostic tool, AXA + Airbus Defence
- ➔ Misunderstanding the role of insurance
 - Transfer to insurance is only a step within risk management
- ➔ Misunderstanding their insurance



Source: FERMA. Management Standards.



Traditional policies do not provide peace of mind

- If we look back at the model, losses can be split up into 4 “insurance loss” categories

→ **3. DAMAGE**

TYPE OF DAMAGE TO COMPANIES

- Theft of intellectual property/ commercially sensitive information
- Business disruption/interruption
- Data and software deletion/destruction
- Direct financial loss:
 - Theft of funds
 - Extortion payments
- Third-party liabilities (customers, employees, shareholders’ actions,) and regulatory actions:
 - Disclosure of third-party data
 - Other
- Reputational loss
- Physical damage:
 - People
 - Physical assets
- Investigation/response costs

• 1st party financial losses

Cover of Standard property policies ... but standard exclusions apply to loss of data

Fines are excluded. Loss of Intellectual property not insurable a priori. Business interruption would not be covered following a non covered event, only as a consequence of covered material damage.

• 3rd party financial losses

Cover of standard liability policies, but pure financial losses often excluded if they are not a consequence of a covered 3rd party bodily injury or property damage. Possible E&O or D&O covers

• 1st party property damage or bodily injury

Bodily injury probably covered either on EL, WC or Accident
Property damage probably covered under standard property policy if no specific cause exclusion. Data is not physical

• 3rd party property damage or bodily injury

Liability policies might provide cover in some cases but cause exclusions will apply

- Specific exclusions apply
- Normally no explicit cyber cover, leading to need to claim based on tacit cover -> uncertainty and litigation
- Even if type of loss is within insurance scope, causes will lead to exclusions
- No specific sum insured in function of the risk

Peace of mind requires risk management and a comprehensive insurance solution

Need for specific insurance that can take away loss and cause discussions, offering typically and with specific sums insured, risk analysis and claims handling:

Property Cover:

- ➔ Remediation costs following the loss or breach of data
- ➔ Business interruption
- ➔ Financial loss following fraud / misappropriation

Cyber Liability

- ➔ Consequences on third parties

Privacy data protection

- ➔ Notification costs
- ➔ Regulator investigation costs

Crisis management

- ➔ Communication costs
- ➔ Legal defense
- ➔ Loss of reputation
- ➔ Identity theft

- In some countries: fines and ransom can be covered.
- Not insurable: theft of intellectual property
- Globally: data breach oriented

Cyber at AXA

- Cover in place
- Offer in place for large companies
- Specific offers in place in France & Germany. Launch imminent in some other countries

Geschäftskunden

Ich möchte, dass unsere Unternehmens-IT vor den Folgen von Cyber-Risiken geschützt ist.

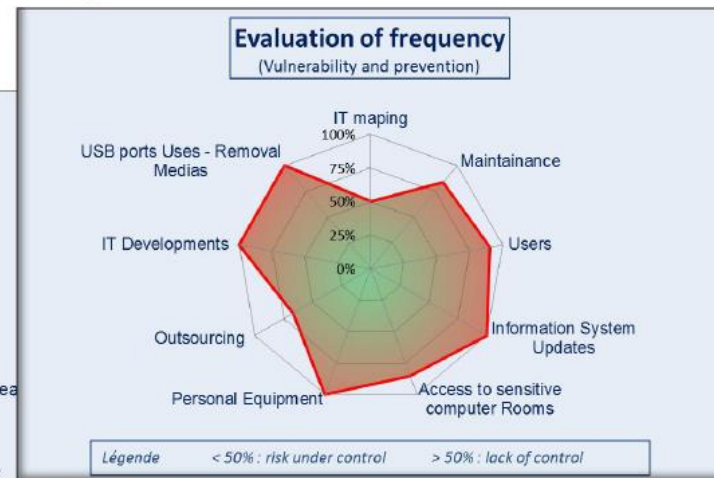
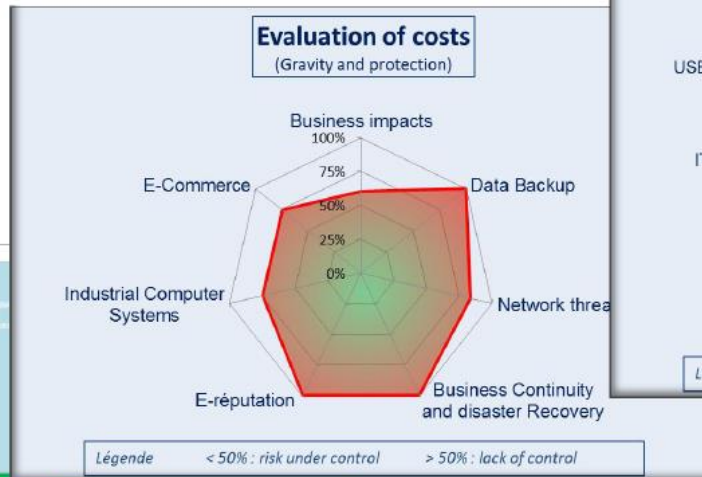
ByteProtect
Cyber-Versicherung für mittelständische Unternehmen

Cyber Sphere

Solutions AXA pour les entreprises

Conditions Générales
CYBER SECURE

Providing risk assessment and analysis:



Product development

Spain:

- ➔ Specific liability policies for IT companies
- ➔ Defense solutions
- ➔ Cyber policies under development:

0. Initiation	Design		Build	Deploy		Monitor	
	1. Market Analysis	2. Technical Analysis	3. Offer Production	4. Deployment Preparation	5. Launch	6. KPIs follow up	7. Improve Offer
0.1 Pre-select potential segment	1.1 Clients Data	2.1 Identify and assess risks of client segment	3.1 Contractual documents	4.1 Prepare distribution	5.1 Communicate on Offer		
0.2 Select Expert Offer team	1.2 Market Data	2.2 Run actuarial studies	3.2 Underwriting Management	4.2 Train & engage	5.2 Offer Go Live		
0.3 Launch process	1.3 Competition Information	2.3 Define offer	3.3 Policy Management	4.3 Prepare communication & marketing	5.3 Post Go live		
	1.4 High level Compliance/Legal	2.4 Premium calculations	3.4 Claims Management				
	1.5 Analysis Report	2.5 Define local customization of offer	3.5 Marketing Management				
	1.6 Validation for further analysis?	2.6 Analysis Report	3.6 Selling support documents				
		2.7 Offer basics validation	3.7 Global offer validation				
			3.8 Localise contracts and procedures				
			3.9 Global/local offer validation				

Insurance Challenges

To develop our product:

- ➔ Assess Real market opportunity: risk is their but willingness to buy is low
- ➔ Multidisciplinary and comprehensive approach required
- ➔ Pricing: no data available
- ➔ Staff and distributor training

Possible solution: easy and simple product, low cost, low limit for an SME market counting on mutualization but we need a critical mass and accumulation risk is a threat

Some global challenges:

- ➔ Accumulation risk: the mayor re-insurance concern
- ➔ Pricing: lack of data -> flattening pricing -> no compensation for prevention
- ➔ Fast moving environment: Bid data, IoT, ...

Insurance Challenges

To develop our product:

- ➔ Assess Real market opportunity: risk is their but willingness to buy is low
- ➔ Multidisciplinary and comprehensive approach required: difficulty to assess the risk
- ➔ Pricing: no data available
- ➔ Staff and distributor training

Possible solution: easy and simple product, low cost, low limit for an SME market counting on mutualization but we need a critical mass and accumulation risk is a threat

Some global challenges:

- ➔ Accumulation risk
- ➔ Fast moving environment: Bid data, IoT, ...
- ➔ Legal environment: legal question marks and non unified legislation on a global business (EU regulation coming up)
- ➔ Pricing: lack of data -> flattening pricing -> no compensation for prevention

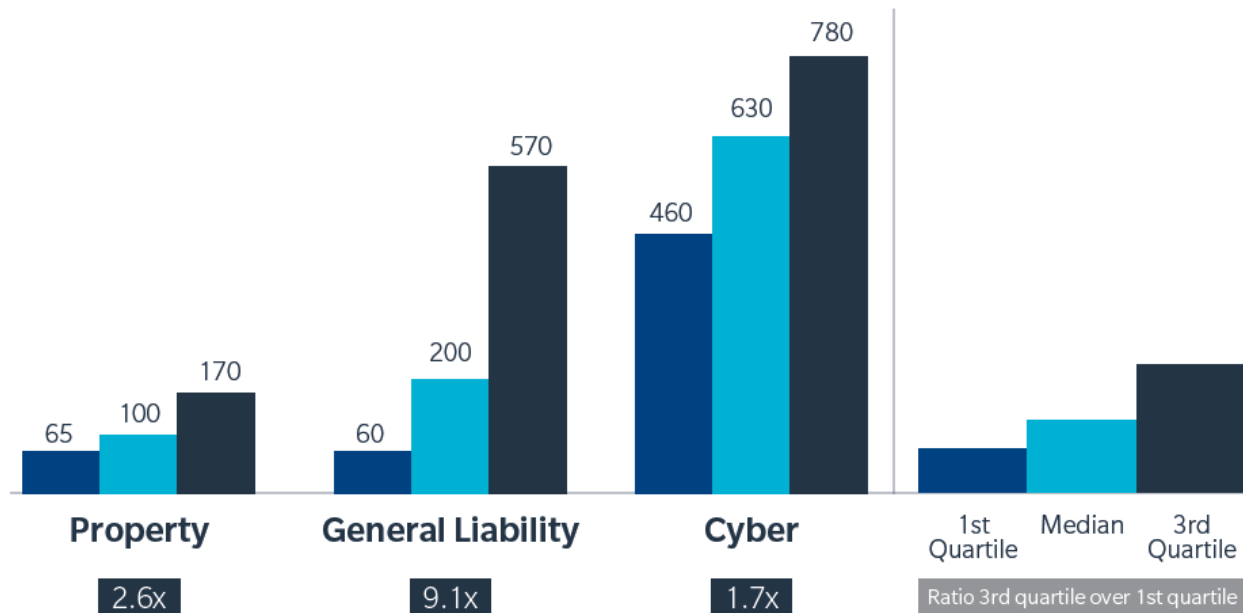
Insurance Challenges

- ➔ Pricing: lack of data -> flattening pricing -> no compensation for prevention

FIGURE 10: PRICING ANALYSIS FOR CYBER, PROPERTY, AND GENERAL LIABILITY

Relative pricing index, property = 100

Based on rate on line for primary layer for companies with turnover <US\$1 billion



Source: UK Cyber Security report

Re -Insurance Challenges & Concerns

➔ Overview of feed-backs

- *Accumulation assessment :*
 - *Definition of the event (on 1st party losses) : duration and extent*
 - *Lack of "premium-to-limit" balance*
- *Understand the insurance market and the technical issues for cyber*
- *Inventory of exposures in dedicated or classical treaties and facultatives (work in progress)*
- *Define key metrics & scenarios to assess the risks, develop an underwriting policy and put in place dedicated capacity for year end*
- *Define a scenario of accumulation to determine their capacity => study in progress (cyber = axis of development)*
- *In the meantime, rather flexible in writings (no strict/specific definition of the cyber event)*
- *Prefer to write separate dedicated treaties (1st & 3rd party)*
- *Currently define strategy & risk appetite : not a uniform approach across departments today*
- *Threats : class action (defense costs)*
- *Other: lack of vision on future strategy; some require already exslusions to renew treaties*

Conclusion

- ❖ Cyber Risk is an increasing and changing risk due to the new digital environment.
- ❖ Risk consciousness is increasing due to the massive use of new technologies and the continuous attacks and problems related to cyber risk.
- ❖ Traditional policies do not provide an adequate level of cover and there is inadequate risk management.
- ❖ For this reason it is necessary to make a new Cyber Risk insurance, but we must face up the following challenges:
 - risk is there but willingness to buy is low
 - Pricing: no data available
 - Accumulation risk
 - flattening pricing -> no compensation for prevention
 - Fast moving environment