Swiss Re

Cyber Risk Insurance

Lutz Wilhelmy, AAE insurance committee, 11 March 2016

Today's journey

1. A definition
2. A market in its infancy
3. Getting to know cyber
4. Actuarial Involvement
   - Taxonomy
   - Costing
   - Accumulation
5. Q&A

Cyber Risk – One Definition

A definition of Cyber

"Cyber risks" are any risks that emanate from dealing with electronic data including its transmission.

This encompasses

- any liability arising from a failure to maintain the confidentiality, integrity and availability of electronically stored information - be it related to individuals, companies or governments.
- loss or corruption of data and its financial consequences,
- physical damage caused by cyber attacks,
- fraud committed by misuse of data,

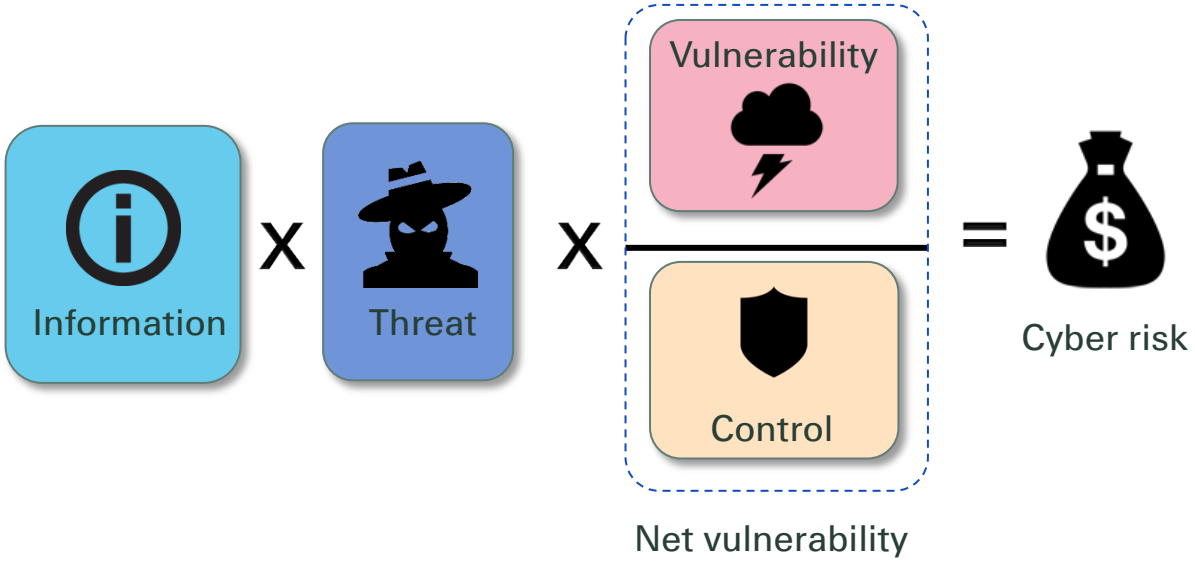
Cyber risk insurance addresses first and third party risks associated with e-business, the Internet, networks and network security and informational assets.

How to assess cyber risks, broadly?

CYBER RISKS

any risks that emanate from dealing with electronic data including its transmission

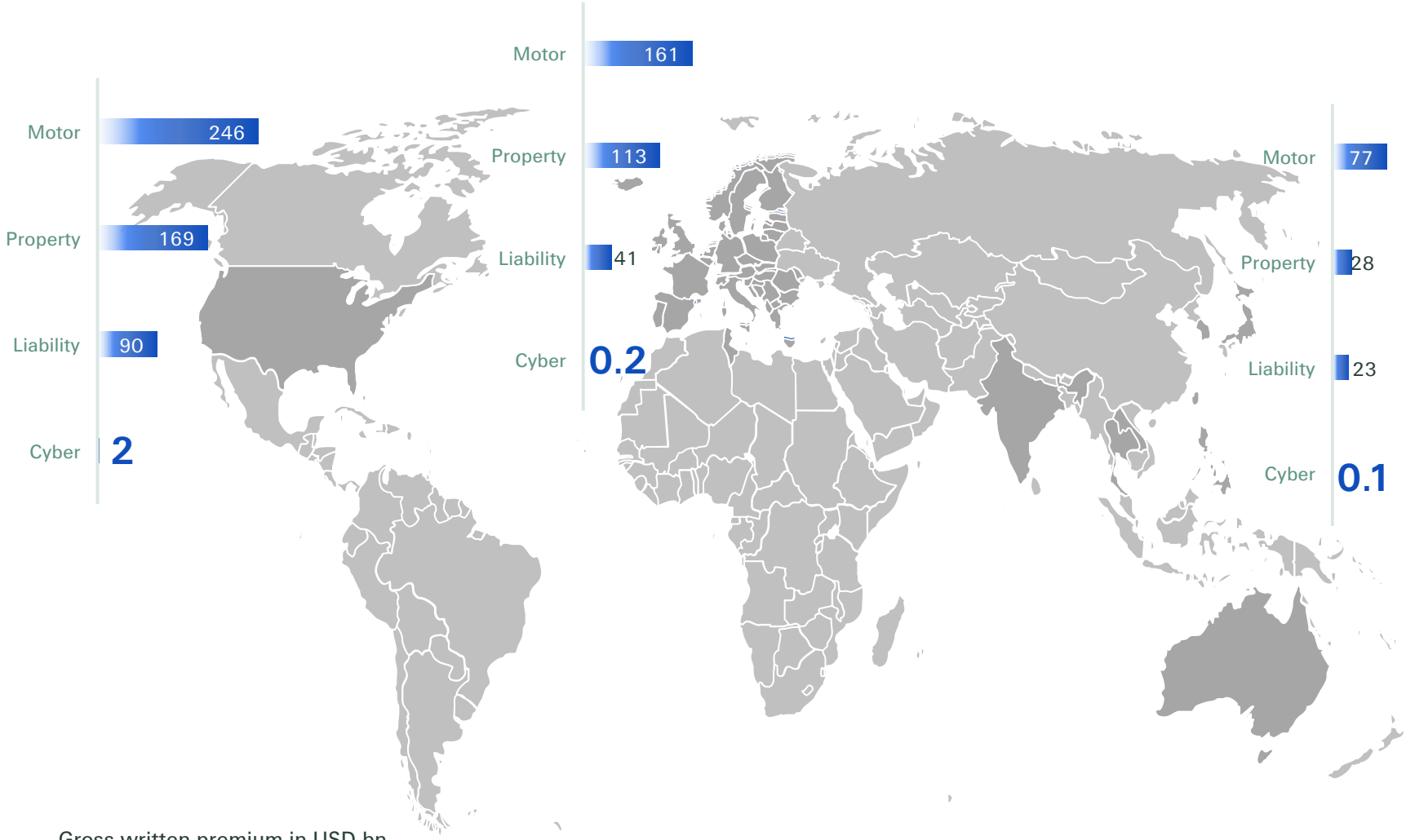
- Naively a combination of four components



- Vulnerability and control is not just about technology but also determined by the people, data handling and business processes involved

A market in its Infancy

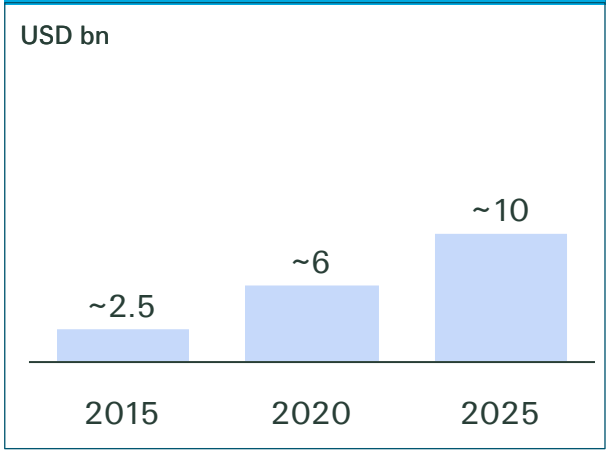
The cyber insurance market is still in its infancy...



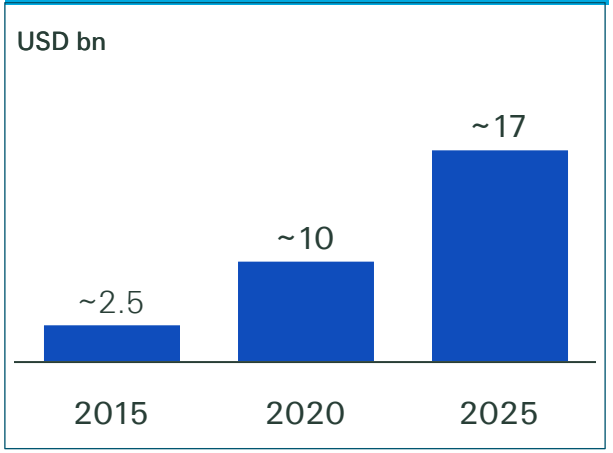
Gross written premium in USD bn
Source: Swiss Re Economic Research & Consulting

We see three main scenarios for the premium growth of the cyber insurance market

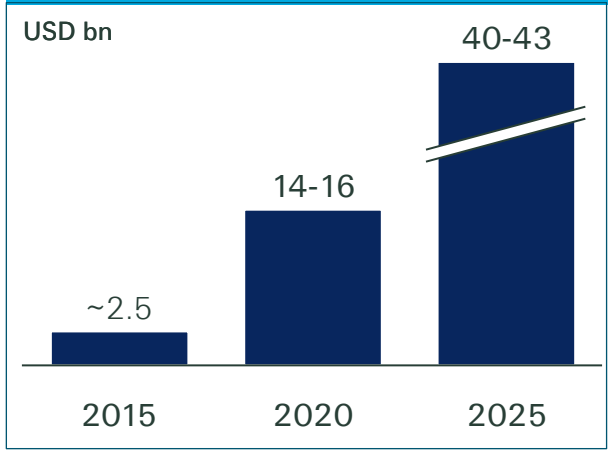
Slow-growth scenario



Base-case scenario

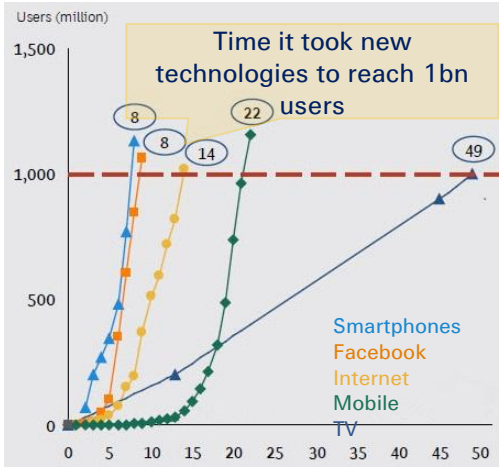


High-growth scenario



Scenario assumptions: heightened threat intensity, heightened awareness, more sophisticated cyber defence, no industry or economy crippling worst case event (1:1000yrs)

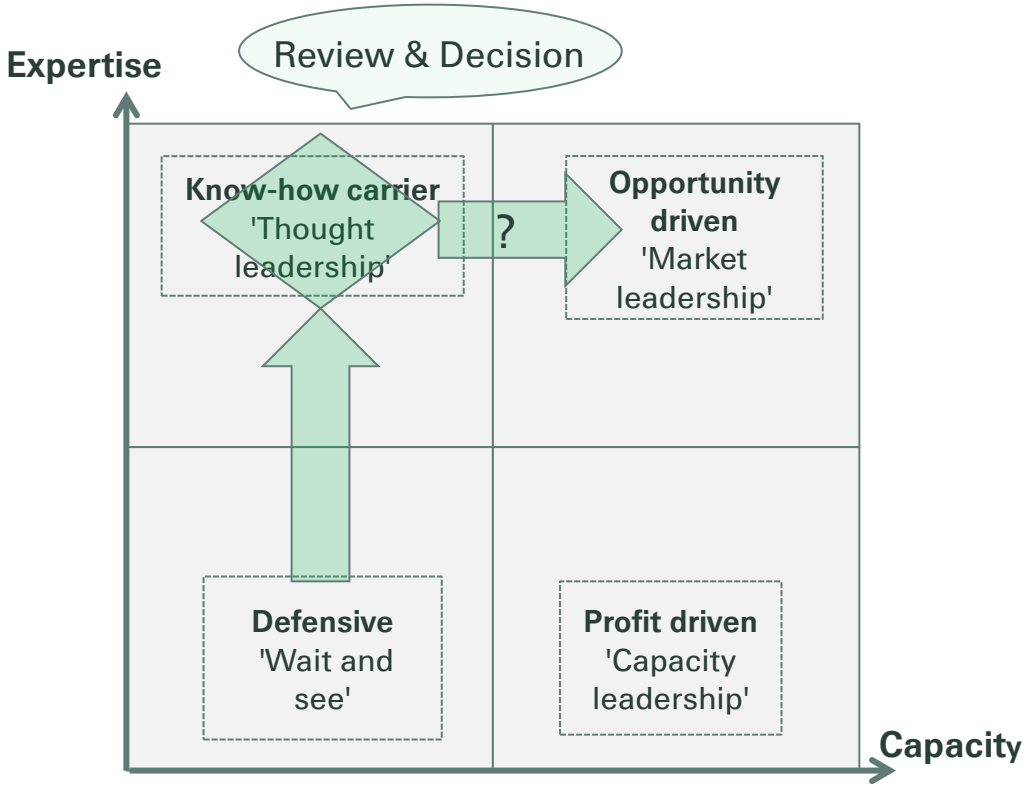
We expect rapid growth in cyber + growth in exposures



Source: BCG

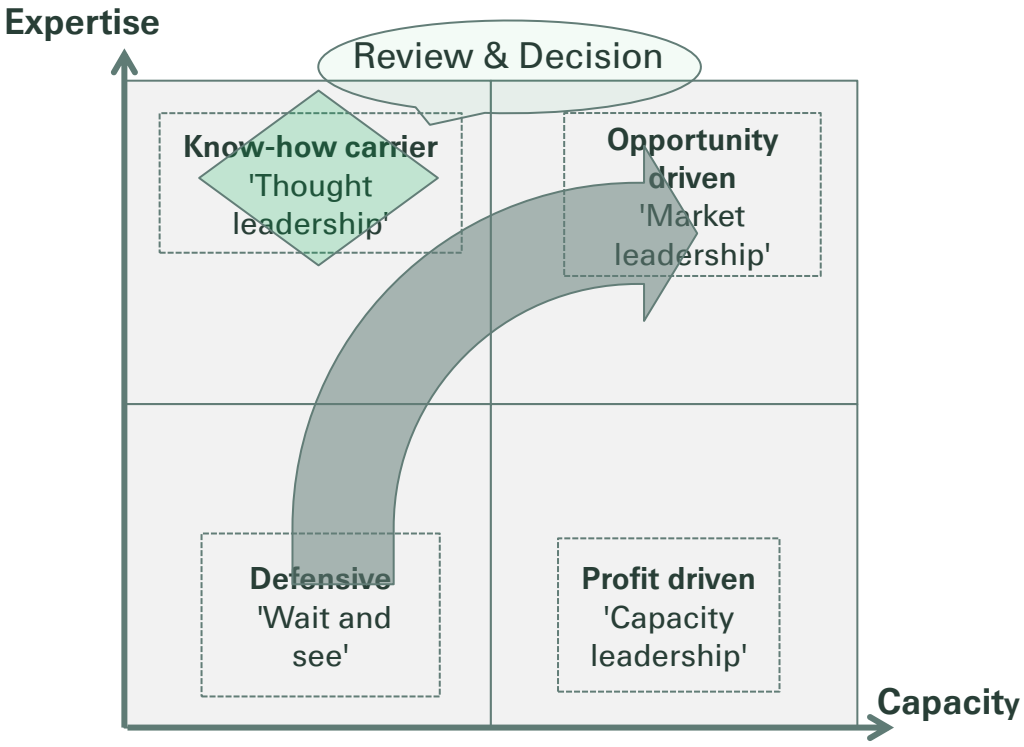

Getting to
Know Cyber

A classical approach to cyber underwriting



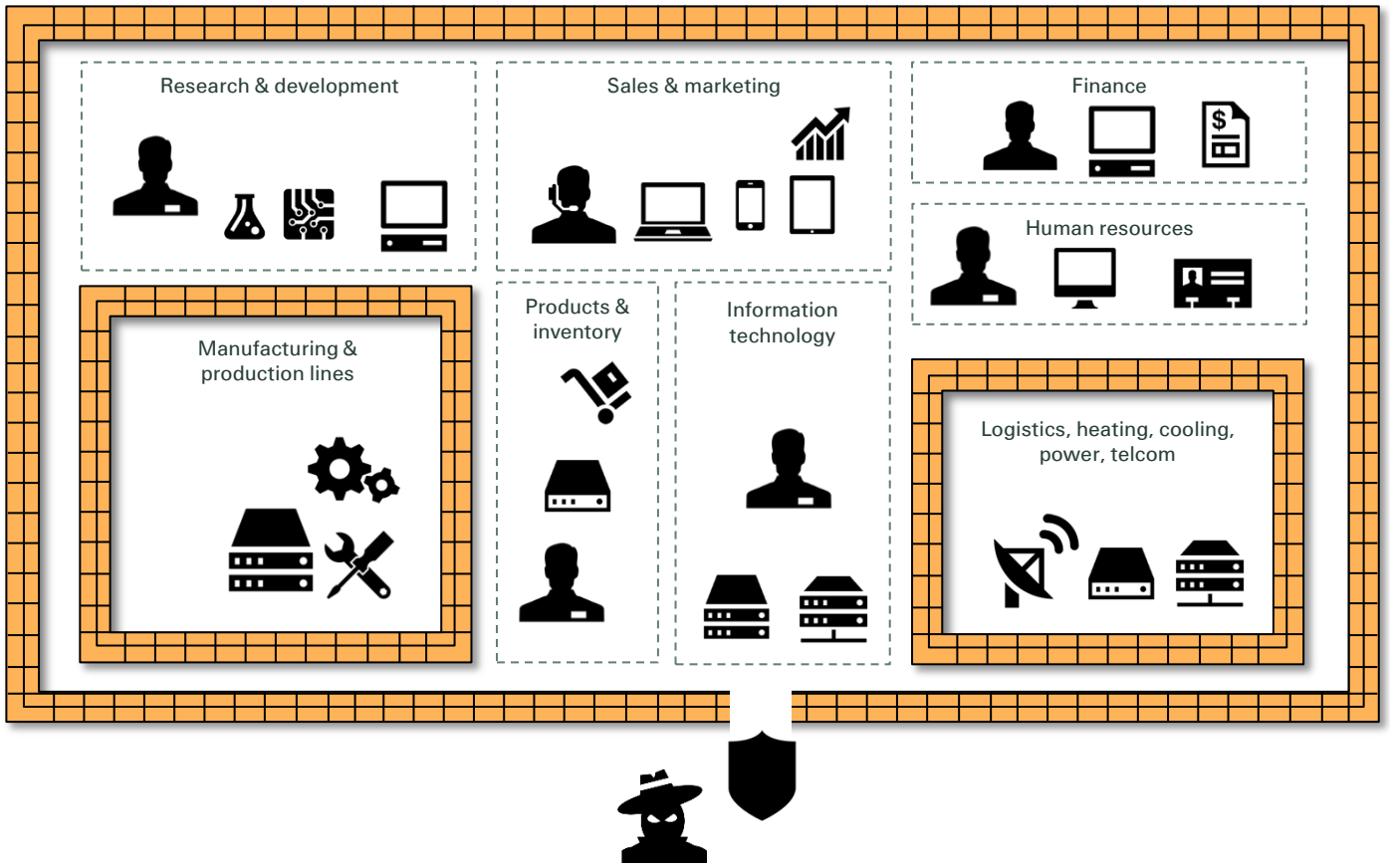
We first aim at building expertise ("thought leadership")
Later we will decide whether we want to achieve "market leadership".

A (more promising?) approach to cyber underwriting

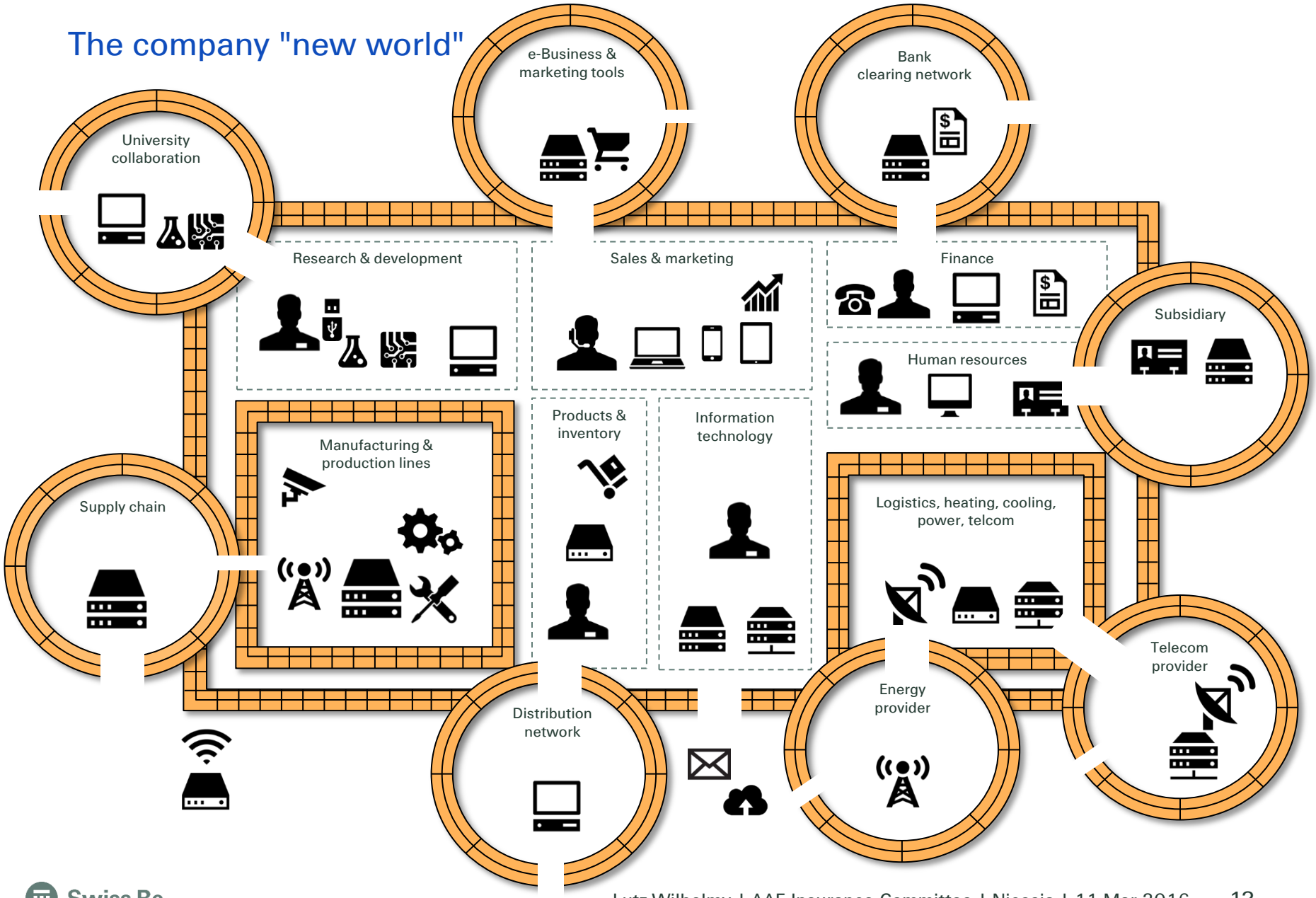


We first aim at building expertise ("thought leadership")
Later we will decide whether we want to achieve "market leadership".

The company "old world"



The company "new world"




SUZUKI
JLX
AAE 787

Actuarial Involvement


Taxonomy

Categorisation/taxonomy of Cyber (Swiss Re)

1) Actions (vector):

- Malicious IT attack
  - external or internal
    - virus* / worm* / malware*
    - phishing/soc. engineering
    - flooding
    - hacking
- Stolen PC
  - and use the key
  - and misuse the data
- Stolen data carrier (USB/HD)
- IT non-malicious - person
  - handling (data, program)
  - programming
- IT non-malicious - machine
  - random error (cosmic ray)
  - overheating of hardware
  - mechanical (hard-disc crash)
  - faulty design
- Physical damage (eg. cable)
  - malicious
  - non-malicious

* generic vs. dedicated, targeted or « cloud »

2) Impact (effect):

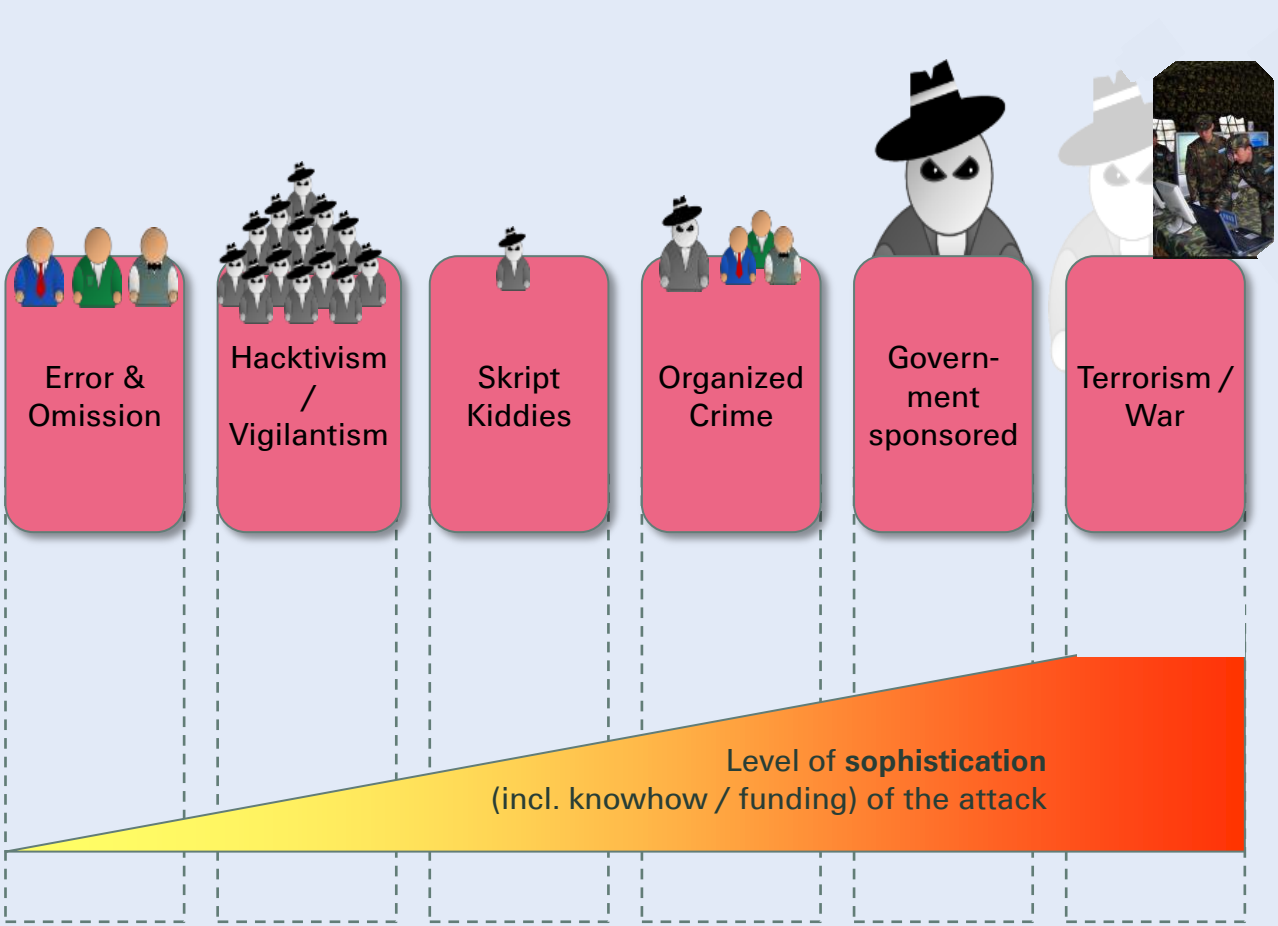
- Data
  - stolen (but not deleted)
    - exposed
    - extortion
    - sold
  - deleted
    - extortion
    - deleted
  - encrypted (extortion)
  - corrupted
    - corrupted
    - extortion
  - exposed
- Business Interruption
  - DoS
  - IO - Interruption Operation (System/Network Interruption)
- Physical damage (SCADA, DCS) (incl. ensuing Bodily Injury)
- IO on medical devices
- Infrastructure down (Electricity, Internet)
- Reputational damage
- Cyber Fraud/Crime

3) Motivation and actors (internal & external):

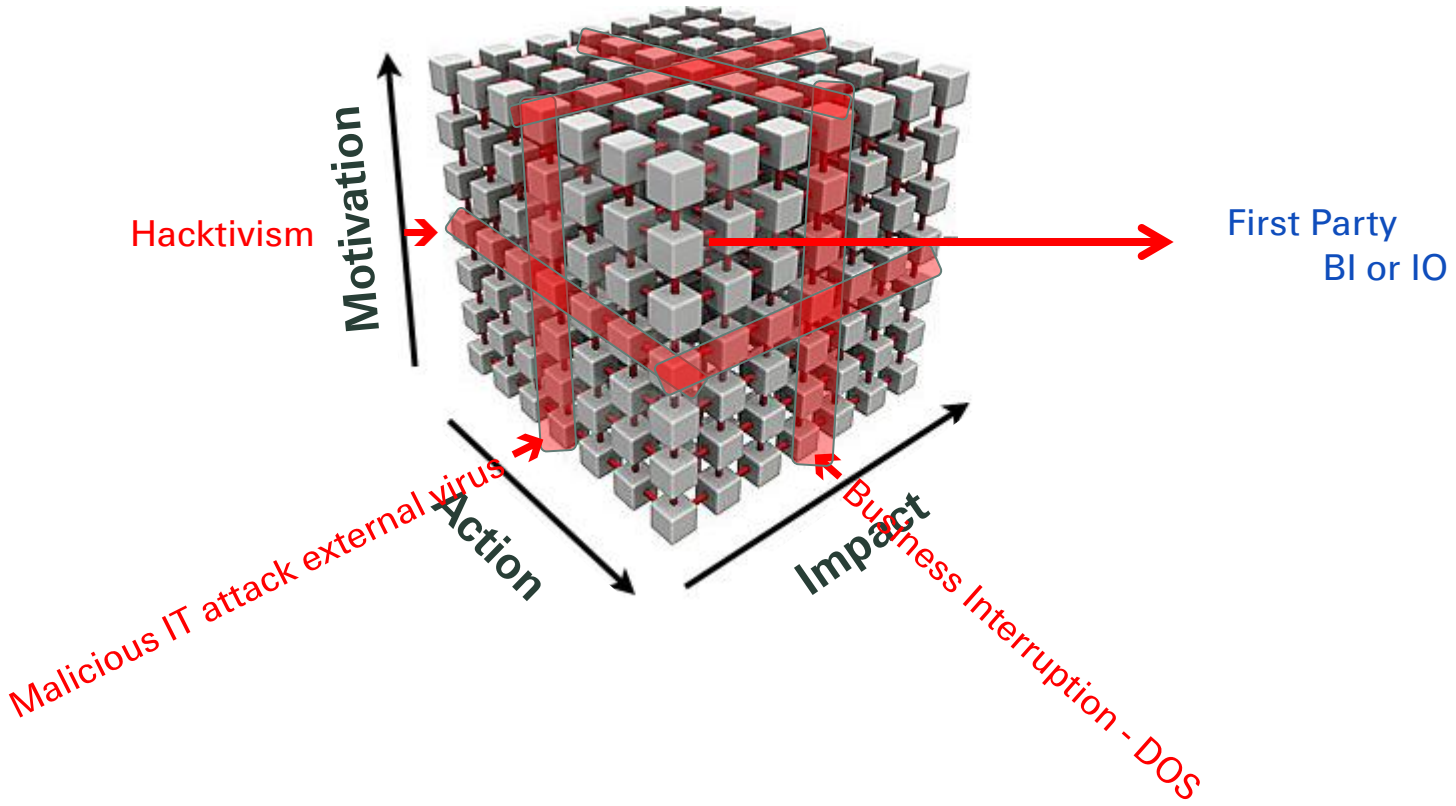
- non-malicious/error (employee / contractor)
- fun, "me too" (script-kiddie)
- hacktivism (social, political)
- revenge
- enrichment
- espionage
  - political (inter-party)
  - government based
  - economic
- terror
  - fear
  - financing
- war
  - declared
  - not declared (conflict)

... another view at actors and motivation ...

Actors & motivation and level of sophistication



Categorising the risks in a data cube



Categorisation/taxonomy of Cyber (Swiss Re)

Insurance solutions:

- First Party
  - BI or IO
  - CBI connectivity
  - reinstatement of data (DR)
  - investigation/crisis mgt.
- Extortion
  - ransom
  - investigation costs
- Privacy (breach)
  - liability (def. & settlement)
  - crisis mgt* (investigation, notification, public relation, credit monitoring)
  - fines & penalties (tbd)
- Network security liability
- Tech E&O
- Communication & Media liability
- Intellectual Property (IP)
- Reputational Damages

Non-affirmative covers:

- Property
- Engineering
- Liability
- Liability PI
- D&O
- etc.

* = incident response costs.

Work in progress: Categorisation according to: Confidentiality / Integrity / Availability

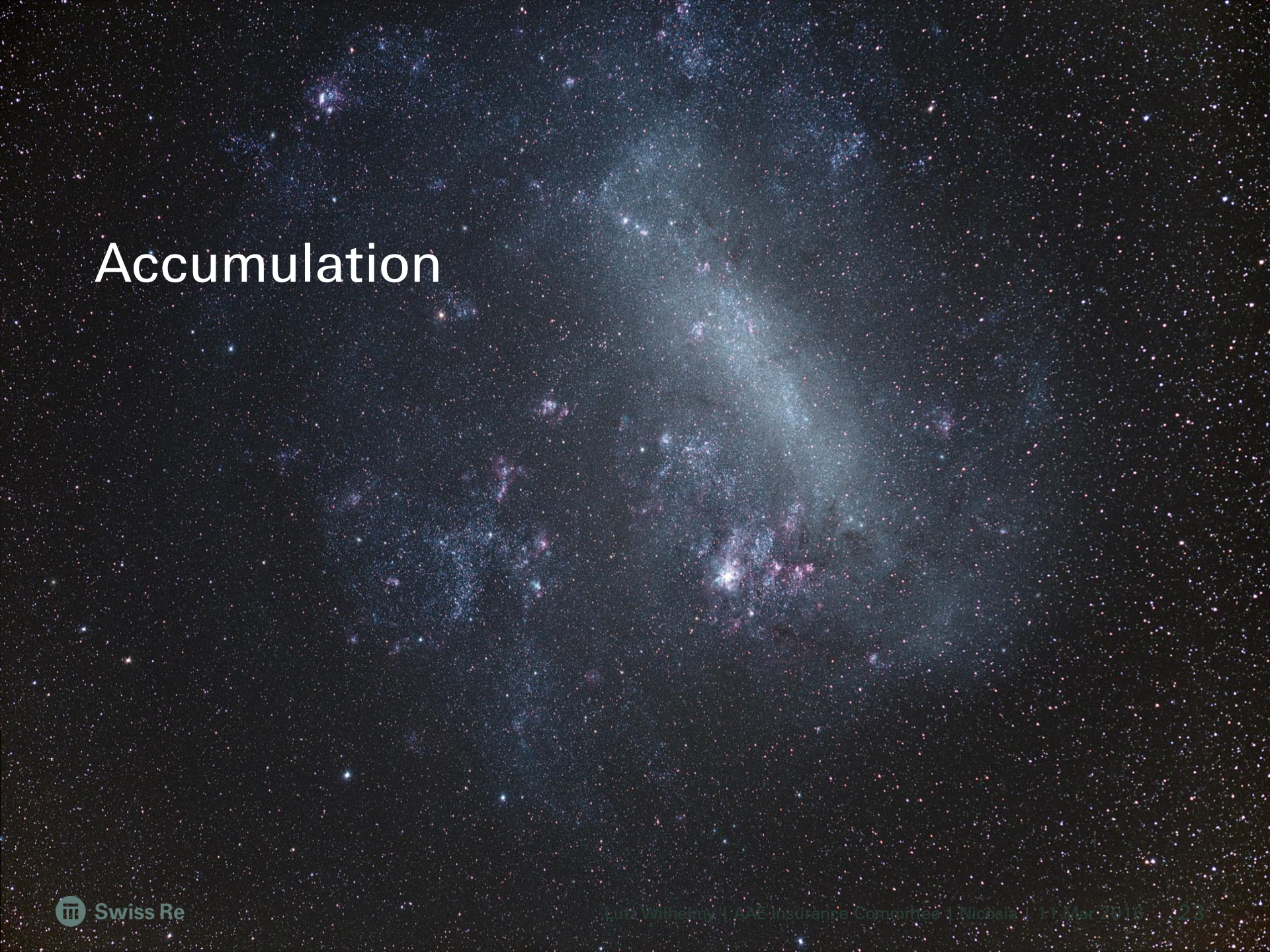
Impact: (assumption = leak is corrected immediately after discovery)

- Data
  - stolen (but not deleted)
    - published ➔ confidentiality
    - extortion ➔ confidentiality
    - sold ➔ confidentiality
  - deleted (but not stolen)
    - extortion ➔ threat (on all three)
    - deleted ➔ availability
  - encrypted (extortion) ➔ availability
  - corrupted
    - corrupted ➔ integrity
    - extortion ➔ integrity
  - exposed ➔ confidentiality
- Business Interruption
  - DoS ➔ availability (of services)
  - IO ➔ availability (of systems, operations), possibly integrity

- Physical damage (SCADA, DCS)
- IO on medical devices
- Infrastructure down
  - Electricity
  - Internet

Costing

Accumulation



Outside Views on Cyber Accumulation Risk

Speaking at the event, Stephen Catlin, Executive Deputy Chairman of XL Group, said governments need to step in and provide a backstop for cyber insurance.

"I have never said that we should not insure cyber, but it is the biggest single systemic risk that I have seen in my career," he told delegates.

Unlike other large risks, such as natural catastrophes and terrorism, cyber is a global, rather than a regional, risk, according to Mr Catlin. He believes that the economic cost of a major global internet outage would easily exceed the capitalisation of the world's property and casualty industry.

"The idea that [the insurance industry] can cover that is asinine," Mr Catlin told delegates at AM Best's Europe Insurance Market Briefing held yesterday.

Cyber accumulation risk is a growing concern in the industry.

Therefore without the governmental back-stop and the industry's ability to address/absorb these risks in the marketplace through traditional insurance products and risk transfer methods, cyber risk has become a factor for rating agency evaluations:

- Fitch Ratings recently stated that "the potential for any future credit impact to major providers is kept in check by the still relatively small size of the cyber-related insurance market." Fitch also noted that it is "less clear how loss aggregation could play out under a severe cyber-attack that leads to insurable events covered by non-cyber related catastrophe policies, including standard commercial liability, business interruption and professional liability."
- A.M. Best indicated that it will ask:
- Specific questions on cyber risk on its Supplemental Rating Questionnaire.
- How the policy is sold - whether it is standalone or as a sublimit within another policy.
- Enquire about lines of business and types of coverage purchased, such as business interruption or theft of cyber assets.
- In meetings with rating analysts, there will be questions, such as whether the client has ever been the target of a cyber-breach or attack and where responsibility lies within the organization when it comes to managing cyber related risks. There will also be a focus on premium and loss expectations for cyber risk as well as estimated costs for crisis services and legal defense (1).

With the increased scrutiny from these types of outside institutions, (re)insurers will need to quantify and address these questions in the future to ensure they are viewed favorably.

Lloyd's has warned about the problem of risk aggregation around cyber a number of times. According to the trade press, a 9th September letter from Tom Bolt informed syndicates of some changes to the risk management regime around this, as the market attempts to better understand its overall exposure.

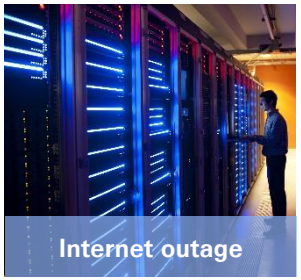
From 1Q16, each syndicate will need to provide quarterly gross aggregations of exposures to cyber attack risk. Specific risk appetite limits would also need to be submitted for cyber, and approved by boards. A more detailed approach is to be developed in conjunction with the Lloyd's Market Association (LMA) by November 30th. Submissions will form the basis of new RDS scenarios for the market. All managing agents in the market are being asked "to consider including terms in their policies to expressly state whether or not cyber attack coverage is provided and, if provided, the limits for that cover." On policies where cover cannot be expressly excluded, the risk aggregation will need to assume full policy limits are available, for maximum conservatism. This is particularly important in the context of general liability and D&O/E&O policies.

Following on from these new rules, there will likely be an increase in capital requirements for syndicates which are overweight in cyber risk.

Business interruption cyber threat scenarios

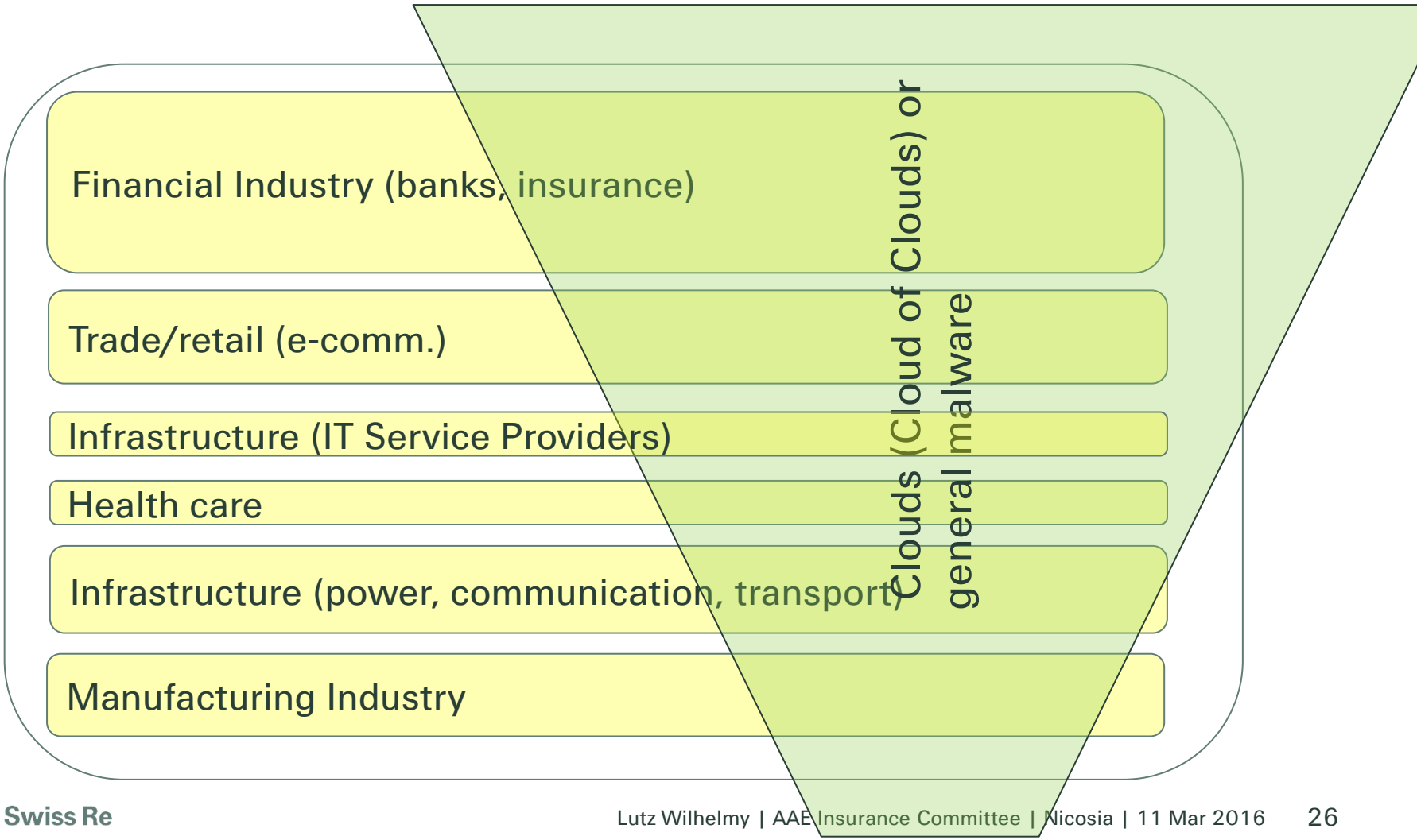

Cloud of clouds outage

- **Generic Scenario 1a:** A hacker group manages to disturb the functionality of a large Cloud of Clouds and delete data. Several main cloud providers are hit, which impacts thousands of users (Data Restoration and BI). The main attack is on clouds situated in North-America with lesser effects on clients located in other part of the world. This scenario is also representative for a major global malware attack.
- **Generic Scenario 1b:** Same as scenario 1a but the main attack is on clouds situated in Europe with lesser effects on clients located in other part of the world.

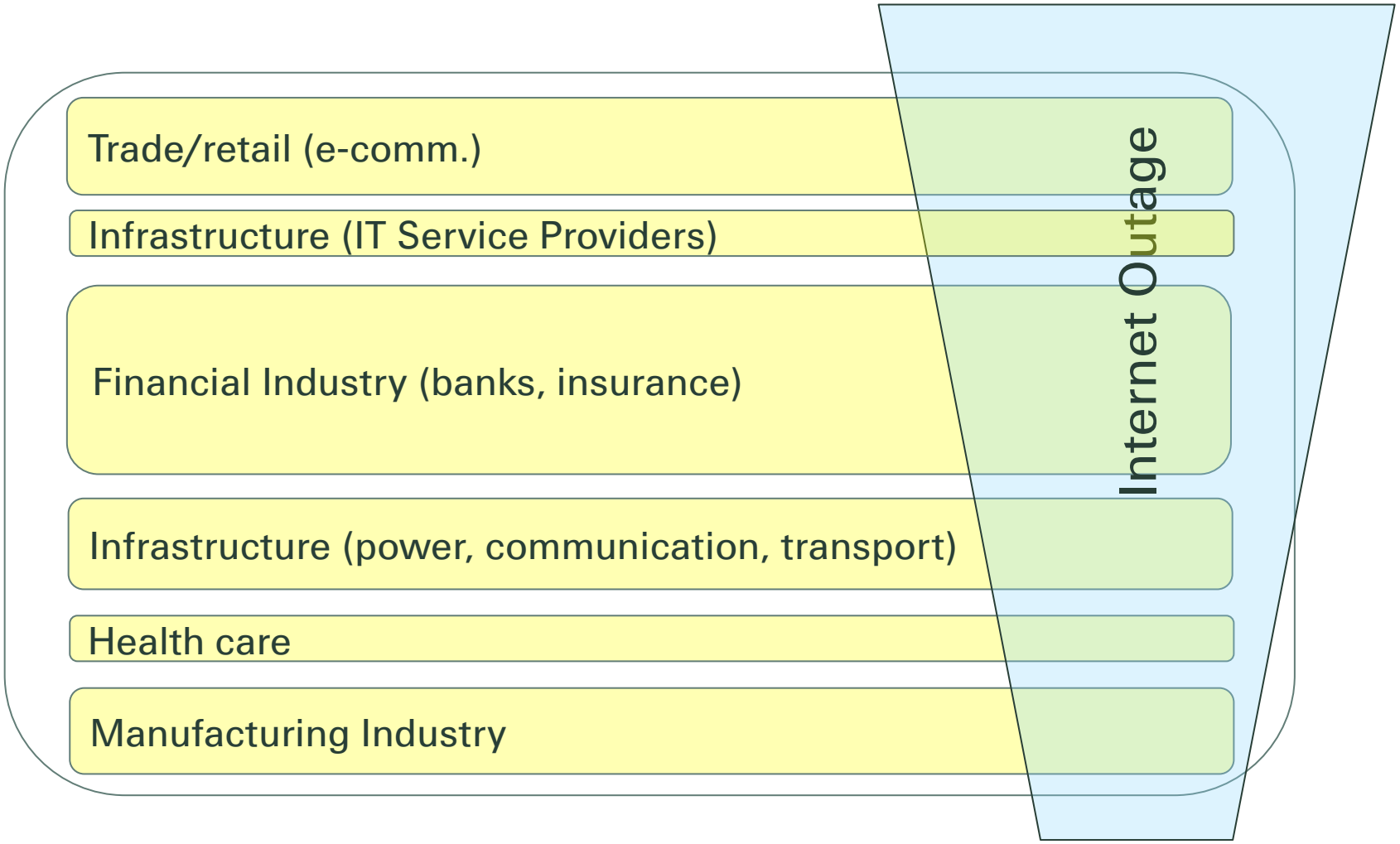

Internet outage

- **Generic Scenario 2a:** A hacker group manages to turn down the Internet for a few days. The main outage is in North-America, with less intense outages elsewhere.
- **Generic Scenario 2b:** Same as scenario 2a but the main outage is in Europe, with less intense outages in other part of the world.

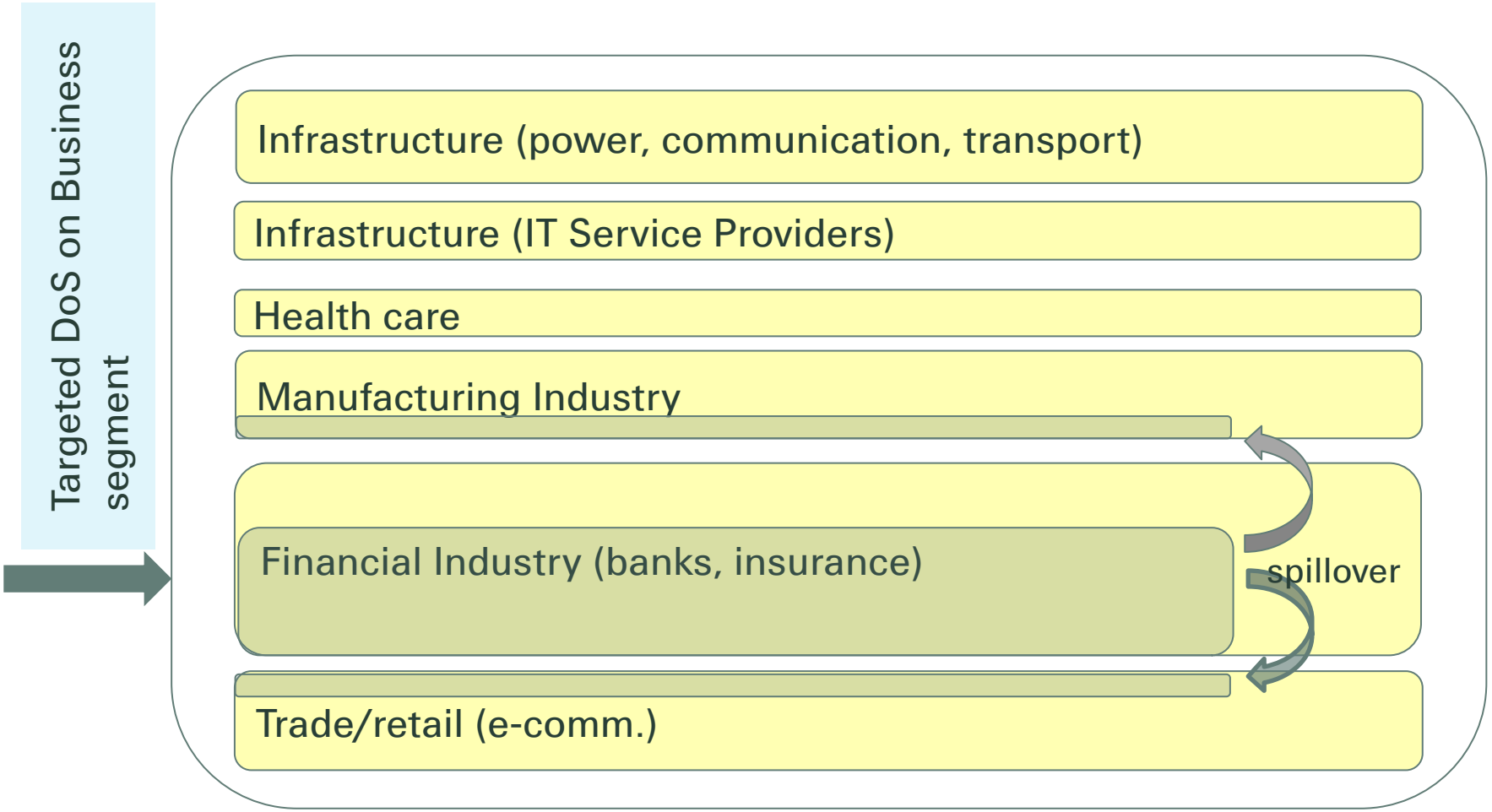
Cyber attack/event on cloud-of-clouds, or General malware attack (non-specific)



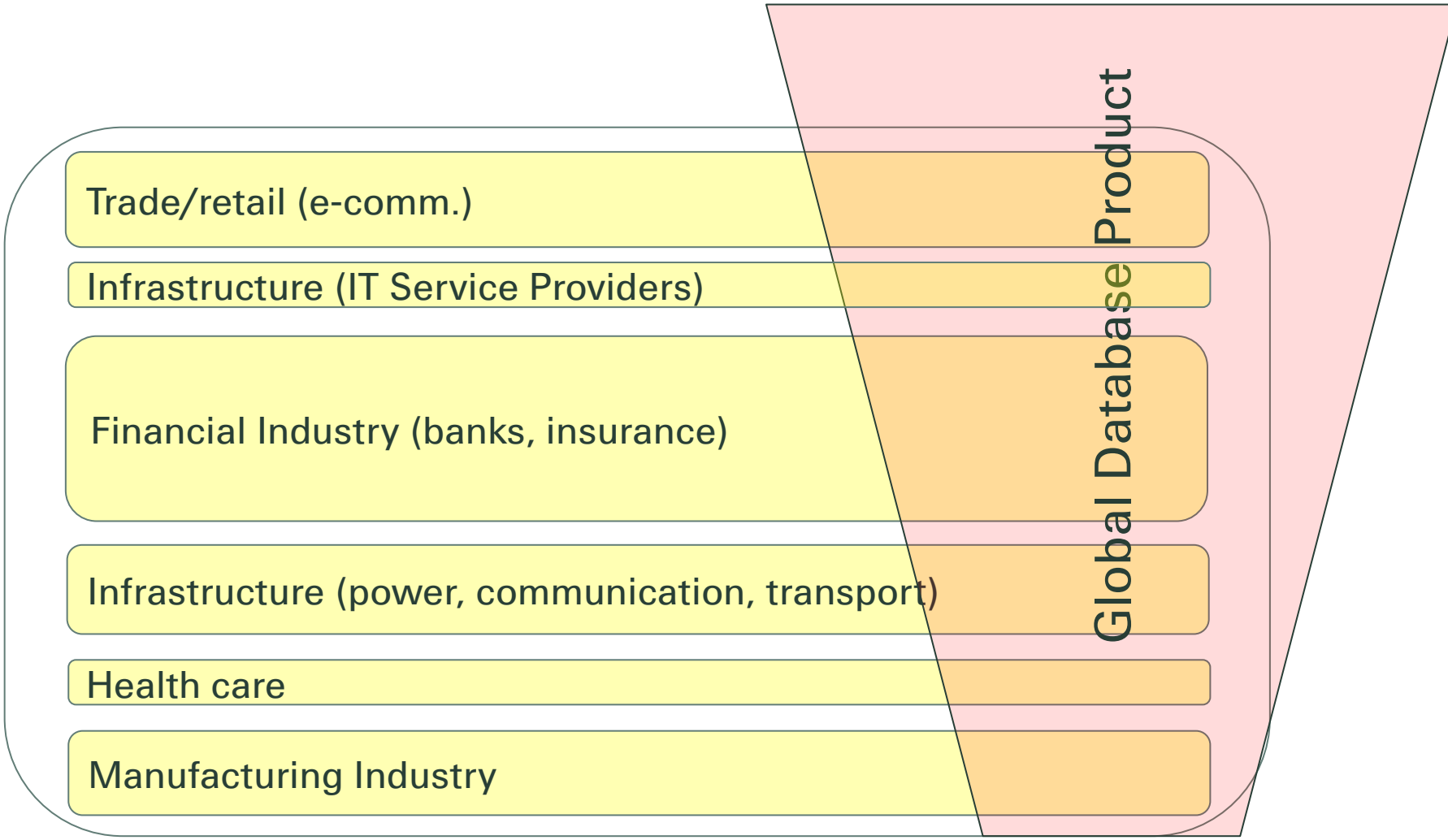
Internet Outage



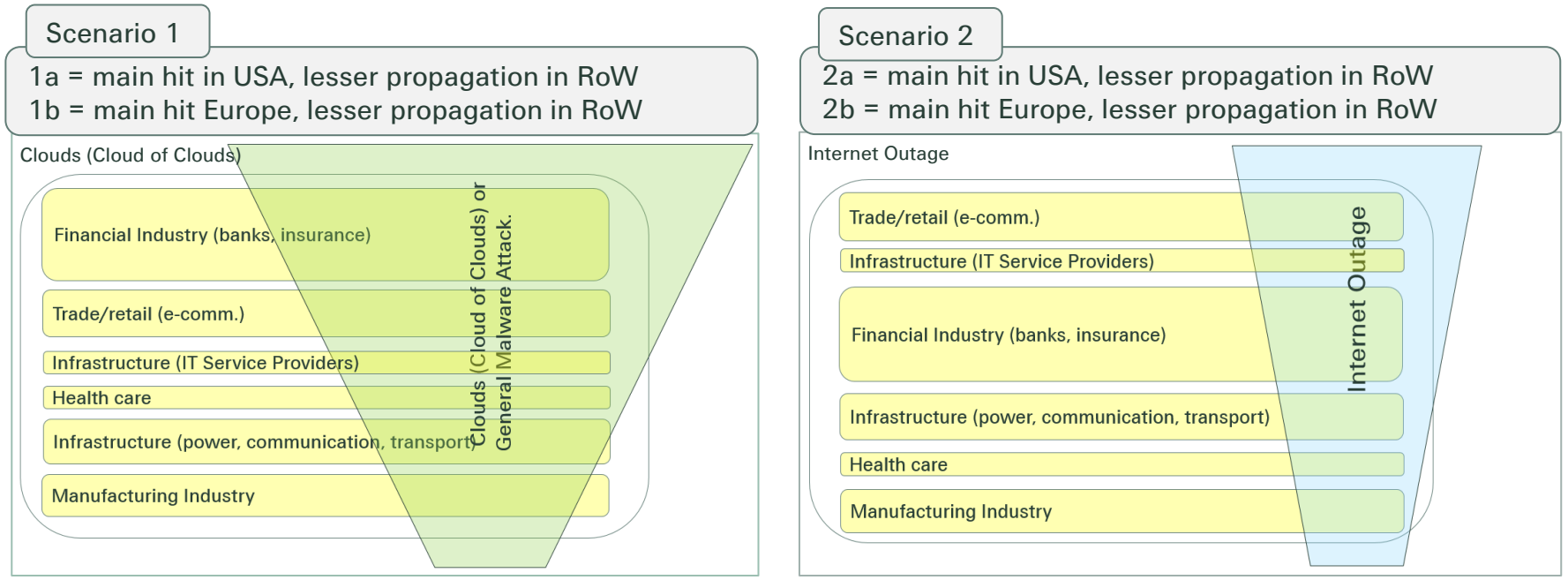
Sub-scenario:
Generic malware attack on a specific industry segment



Scenario of Tomorrow? - PII / FII attack



ISBI/DR approach applied on 2 scenarios



Steps applied to both scenarios:

All treaties explicitly covering ISBI and DR (except treaties excluding all accumulation scenarios)

Calculate the Amount@Stake (function of layer, occurrence limit, ISBI sub-limits, AAL)

Number of policies exposing the treaties

Position of the layer's deductible (versus size of ceded policies for per Risk, versus combination of size and number of policies for per Event treaties)

Business composition (industry segments, geo-split)

Resulting capacity, subject to a minimum capacity charge (on A@S).

Application to a specific Global Cyber Quota Share

All treaties explicitly covering ISBI and DR

no coverage restriction to "attacks solely and exclusively targeted at the Insured" -> treaty subject to capacity management

Calculate the Amount@Stake for SR share:

12.5% * 250m = 31.25m EUR

Number and size of policies exposing the treaties:

estimation based on EPI:
ca 30 policies / avg HGI limit ca. 11m (cover fgu)
-> AAL quite remote, apply reduced capacity factor

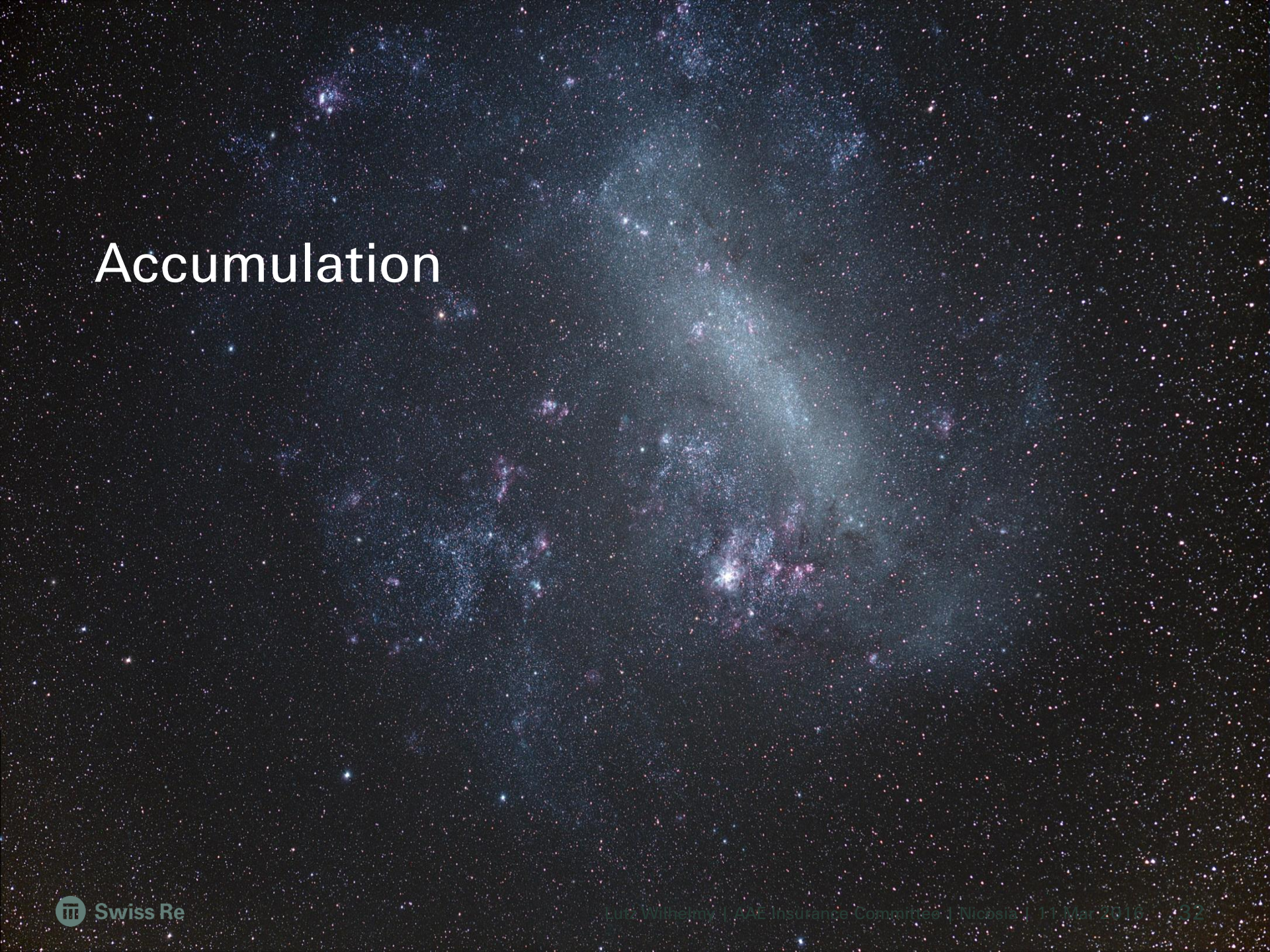
Business segment composition and geo split:

reduced capacity factor due to moderately exposed segment split and no US exposure

Capacity charge reduced from 250m to 54m EUR (100%), net premium to capacity ratio ca 3.3%, but drops below 2% if a loss ratio of 30% "without accumulation events" is assumed

- The current AAL level is high for the (estimated) portfolio size.
- The ratio of estimated net premium to capacity consumption is low.
- A further increase of the AAL would drive up capacity consumption.

Accumulation



Any questions?

Legal notice

The information and opinions contained in the presentation are provided as at the date of the presentation and are subject to change without notice. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the details given. All liability for the accuracy and completeness thereof or for any damage or loss resulting from the use of the information contained in this presentation is expressly excluded. Under no circumstances shall Swiss Re or its Group companies be liable for any financial or consequential loss relating to this presentation.