Prof. Dr. Robert Koch LL.M. (McGill)
Managing Director of the Institute of Insurance Science
Faculty of Law, University of Hamburg

AIDA Marrakech Insurance Conference 2019

Current state of the German cyber insurance market

Agenda

A. Overview of the cyber insurance market in Germany
B. Forerunners of cyber insurance
C. Barriers for the general cyber insurance market
D. Cyber insurance coverage types
E. Silent cyber risks
F. Summary and outlook

A. Overview of the cyber insurance market in Germany (1)

- According to the German Insurer Association (GDV) the German insurance market is the sixth largest in the world in terms of premium income. In 2017, Germany accounted for approximately 4.6 percent of global insurance premiums.
- In 2017, the volume of premiums for the entire primary insurance market in Germany totaled 198 billion Euro.
- Property and casualty insurance accounts for 68.3 billion Euro. No specific data for cyber insurance are published.

A. Overview of the cyber insurance market in Germany (2)

- Cyber insurance market for 2015 was estimated to have a moderate premium volume of 20-30 million Euro (premium volume for business fire insurance is 6 billion Euro).
- Depending on the business 1 mill. Euro coverage for 1.000 Euro annual premium available.
- General perception that cyber insurance market has still low premium volume and only sporadic growth but the President of the German Insurance Association (GDV) recently stated.

"We anticipate exponential growth in this segment, as no company will be able to ignore this risk in the future".

A. Overview of the cyber insurance market in Germany (3)

- For Europe as a whole, AGCS predicts a market with premium revenues of 700 to 900 million Euro.
- Allianz and AXA expect a premium volume of up to 300 million Euro in 2021 in the German segment alone.
- Over the intermediate term (2021), KPMG calculates insurance premium volumes of between 420 and 880 million Euro for business and private insurance customers in the German speaking world. A premium potential of up to 26 billion Euro is predicted for 2036.

B. Forerunners of cyber insurance (1)

- In the 1970ies financial losses suffered by computer abuse and data abuse caused by employees covered under infidelity insurance.
- Since 2000 financial losses suffered by computer abuse and data abuse caused by third parties (incl. cyber attacks) covered under infidelity insurance.
- In the aftermath of the anticipated Y2K losses liability insurance for IT-service provider (mono line insurance).

B. Forerunners of cyber insurance (2)

- Electronic equipment insurance and its extensions of coverage to the recovery of data and software the integrity and availability of which was impaired due to over or under-voltage or damage to the data media (exclusion of cover if caused by software bugs and denial-of-service attacks).
- First cyber insurance policies (stand-alone policies) covering both first and third party property and financial losses (multiline policies) offered in 2011.
- Number of insurers offering stand-alone cyber insurance policies has risen to more than 30.

B. Forerunner of cyber insurance (3)

- March 2017: GDV published non-binding wording for cyber insurance for SMEs.
- Provision of cover not limited to business customers.
  - protection against conflicts arising from the use of the internet and social media or small sub limits to customers' personal area such as identity theft and payment card theft.
- No integration of cyber risk into classic insurance policies through additional modules that are added to existing policies.

C. Barriers for the general cyber insurance market (1)

Supply barely existent
- Actuarial problems
- Lack of sufficient empirical data
- Difficulty in calculating premiums
- Lack of skilled experts
- Cost-benefit issues
- Risk-bearing capacity/ liquidity risk

→

Stagnating growth of the general cyber insurance market

←

Demand barely existent
- Information asymmetry
- Lack of coverage clarity
- Lack of awareness
- Lack of transparency & varying condition schemes
- Cost-benefit analysis
- Negative assessment
- Regulatory-legal
- Complex certification landscape

Source: Brandenburg Institute for Society and Security

C. Barriers for the general cyber insurance market (2)

➢ Types of Non-Demanders in the Cyber Insurance Market

Type 1	Lack of cyber risk awareness, so insurance is viewed as irrelevant.
Type 2	Are aware of cyber risk but regard existing protections as adequate.
Type 3	Are aware of cyber risk, regard existing protection as inadequate, but have a negative assessment of the cost-benefit ratio of cyber insurance.
Type 4	Are aware of cyber risk, regard their existing protection as inadequate, have a fundamentally positive assessment of the cost-benefit ratio of cyber insurance, but barriers (e.g. information asymmetries) exist to purchasing a policy or no appropriate insurance solution is offered by the supply side.

Source: Brandenburg Institute for Society and Security

C. Barriers for the general cyber insurance market (3)

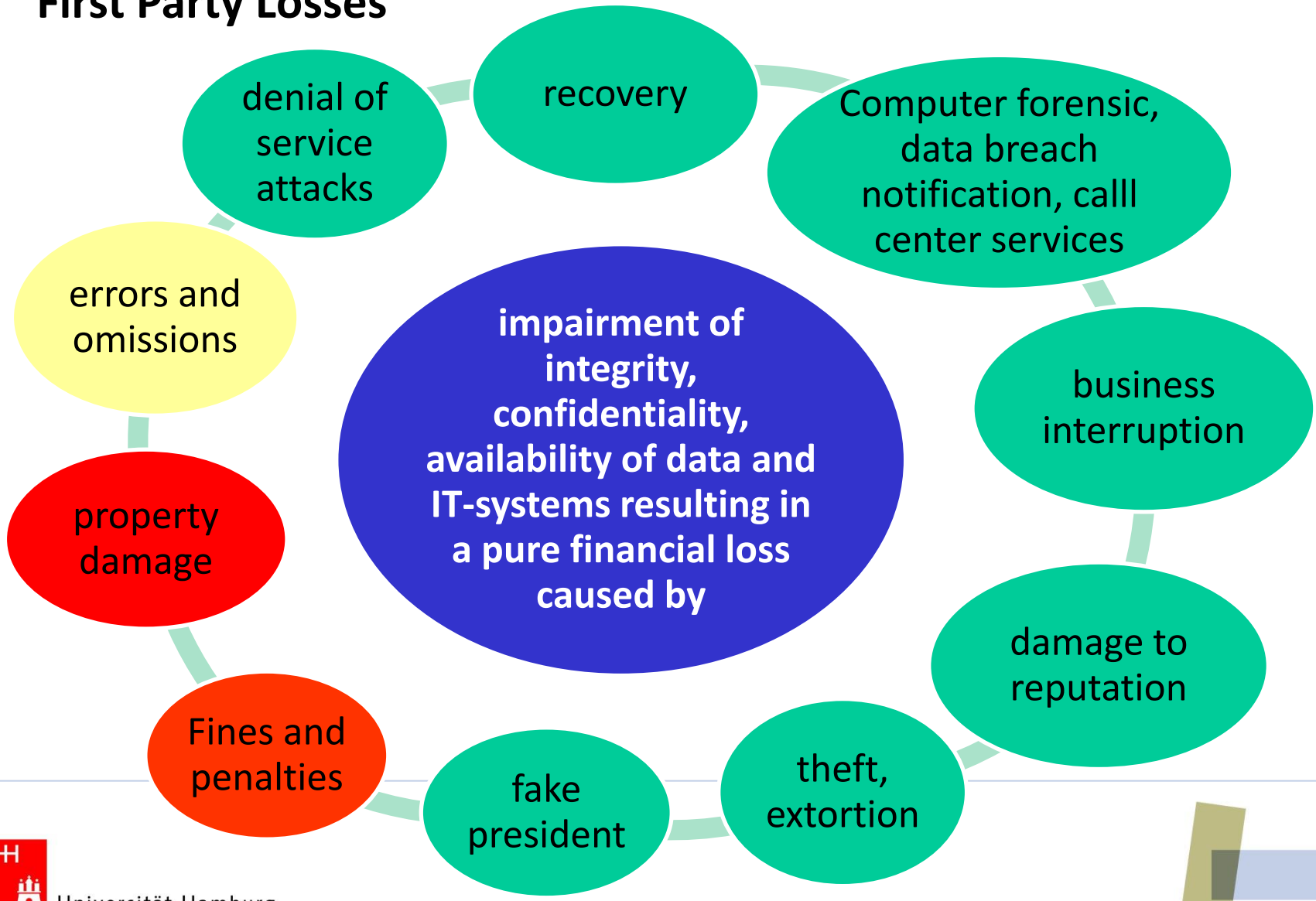
- Lack of coverage clarity and lack of transparency & varying condition schemes.
- Complex wordings (up to 50 pages).
- Different (multi) lines of business bundled.
- Abstract vs. specific description of coverage.
- Costs inclusive vs. costs in addition.
- German market: majority of cyber policies stipulates different definitions for the insured event for the third-party liability and another for the first-party loss cover.

C. Barriers for the general cyber insurance market (4)

- No uniform trigger for third-party liability :
  - Claims made
  - Manifestation of damage (GDV model): the insurance event will be deemed to occur when the damage is verifiably identified for the first time. The identification of the damage can be made by anyone, regardless of his or her relationship to the insured (e.g. experts, third party which suffered a damage or any other third person).

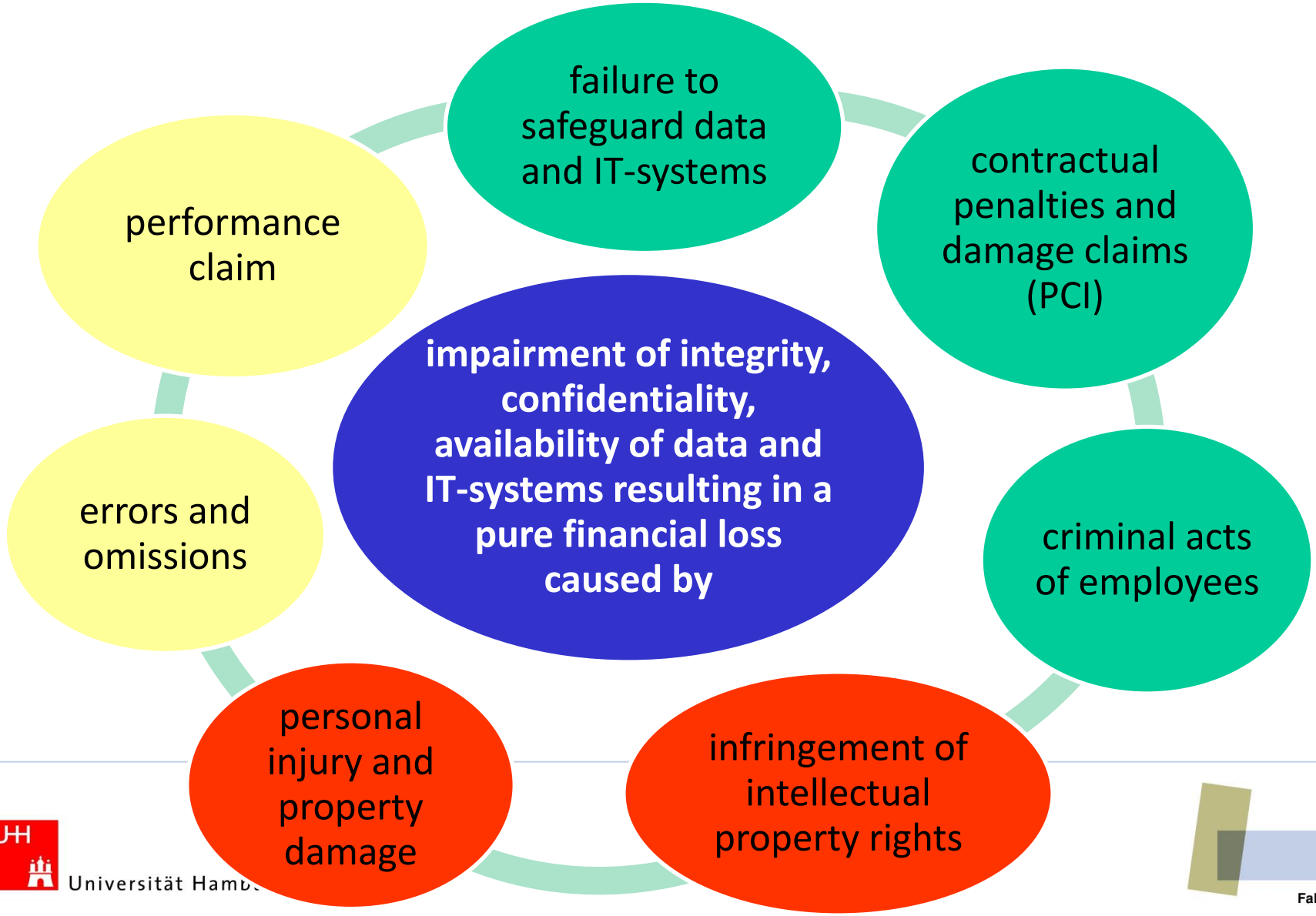
D. Cyber insurance coverage types (1)

I. First Party Losses



D. Cyber insurance coverage types (2)

II. Third Party Losses



E. Silent cyber risks (1)

I. Definition

- Non-affirmative risks (or “silent” risks) refer to instances where cyber exposure is neither explicitly included nor excluded within an insurance policy.
  - E.g.: malware infecting a GPS causing aviation, marine or car accidents; cyber incident causing fire for example through a device connected to houses.
- Non intended exposure to cyber risks.
- Coverage overlap
  - double insurance
  - cumul risks (liability insurance)

E. Silent cyber risks (2)

II. First Party Losses – Overlap of Coverage

- **Named perils**
  - e.g. fire insurance, extended coverage insurance, insurance for business interruption due to fire.
  - data by express definition in the policies ≠ thing
- **All risks (technical insurances)**

  by means of endorsement:
  - coverage for restoring the data of the operating system (e.g. electronic equipment insurance)
  - coverage for restoring all kind of data (e.g. software insurance)

E. Silent cyber risks (3)

II. First Party Losses – Overlap of Coverage

- **Fidelity insurance**

  provides cover against direct losses caused by tortious acts or omissions of trusted persons in a company. Tortious acts include theft, fraud and embezzlement.

E. Silent cyber risks (4)

III. Third Party Losses – Overlap of Coverage

- Professional liability insurance (coverage for pure financial loss)
- D&O insurance (coverage for pure financial loss due to a failure to implement an IT risk management e.g. in accordance with Directive EU 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union)
- Fidelity insurance (coverage for direct financial loss)
- Motor liability insurance (coverage also for pure financial loss)

E. Silent cyber risks (5)

III. Third Party Losses – Overlap of Coverage

- private liability insurance and commercial liability insurance
  - express cover for damages arising from the exchange, transmission or provision of electronic data due to
    - *the deletion, suppression, rendering unusable or modification of data stored with third parties caused by viruses or malicious programs;*
    - *alteration of data for other reasons and the failure to record or to save data;*
    - *disturbance of access to electronic data exchange*

E. Silent cyber risks (6)

III. Third Party Losses – Overlap of Coverage

- private liability insurance and commercial liability insurance
  - cover for damages arising from the violation of personal data protection laws
  - exclusion from coverage for damages arising out of IT service provision activities (eg web-hosting)
  - different triggers (event vs. claims made under many cyber risk insurances)

E. Silent cyber risks (7)

Bank of England Prudential Regulation Authority (PRA) expects that all insurers

- assess and manage their insurance products with specific consideration to non-affirmative cyber risk exposures.
- introduce measures that reduce the unintended exposure to this risk.
- to achieve this, consider any of the following:
  - adjusting the premium to reflect the additional risk and offer explicit cover;
  - introducing robust wording exclusions; and/or
  - attaching specific limits of cover.

F. Summary and Outlook

- German cyber risk insurance market still in its infancy.
- No industry/sector-specific cyber coverage.
- No/little coverage standardization.
- Silent cyber: cumul risks and double insurance.
- Stand-alone policies vs. inclusion of cyber risks in traditional policies?