Cyber Risk and Insurance
Opportunity & Liability

Carsten Topsch

Munich RE

Cyber risk and insurance
Agenda

1. Motivation
2. Munich Re position in cyber
3. Cyber – going into detail (underwriting)
   - Wording
   - Risk assessment
   - Pricing
   - Cyber accumulation exposure for insurer and reinsurer
4. Claims management
5. Munich Re services

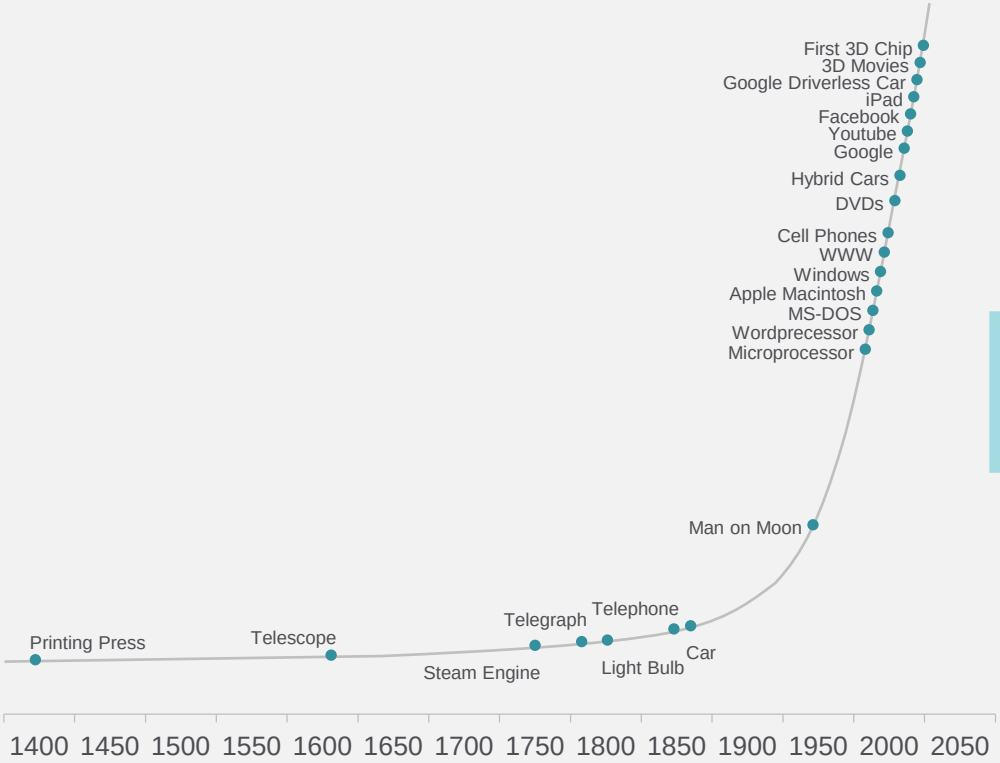
Motivation

Munich RE

Image: used under license from shutterstock.com

Motivation

Accelerating growth in technology

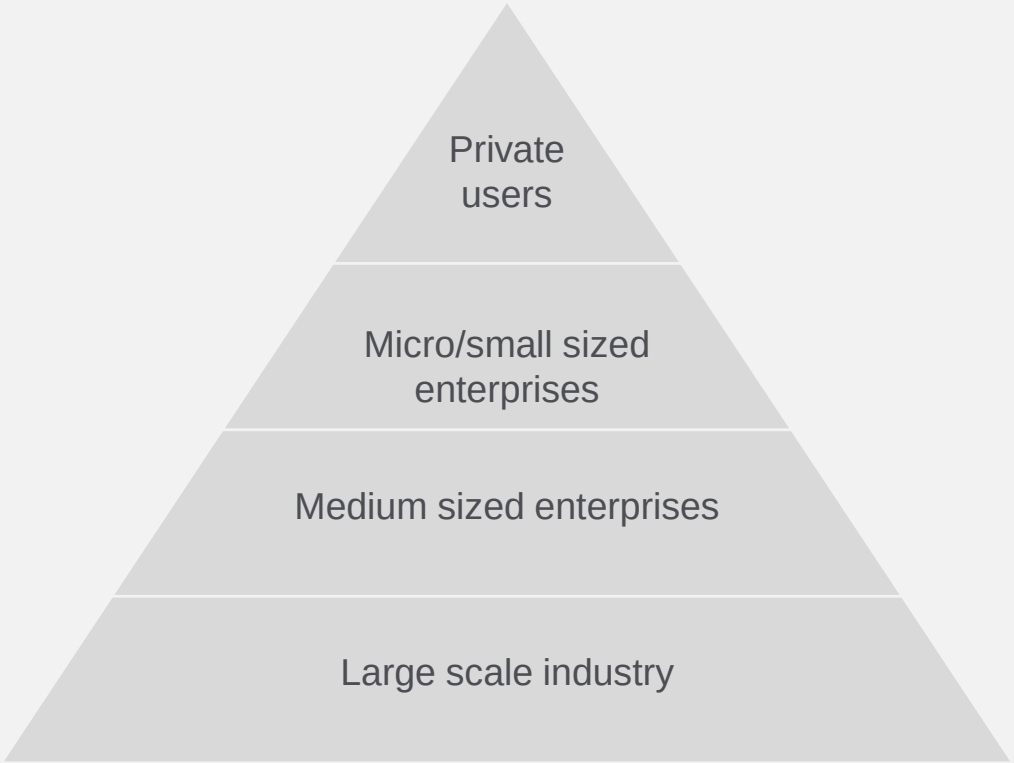


Leads to exponential develop-ment of cyber exposures

Source: asgard.vc

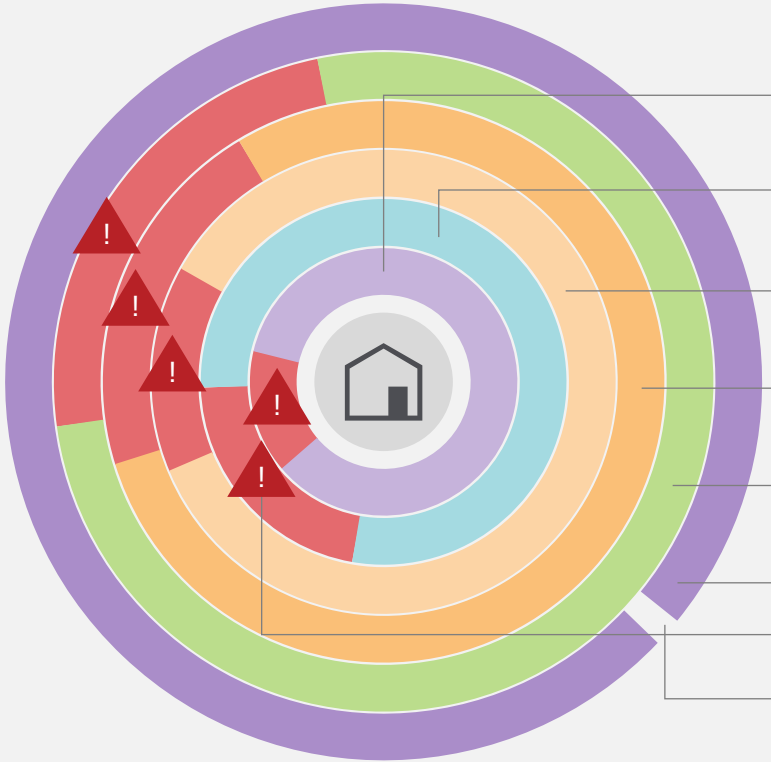
Motivation

Target audience



Motivation

Cyber security framework

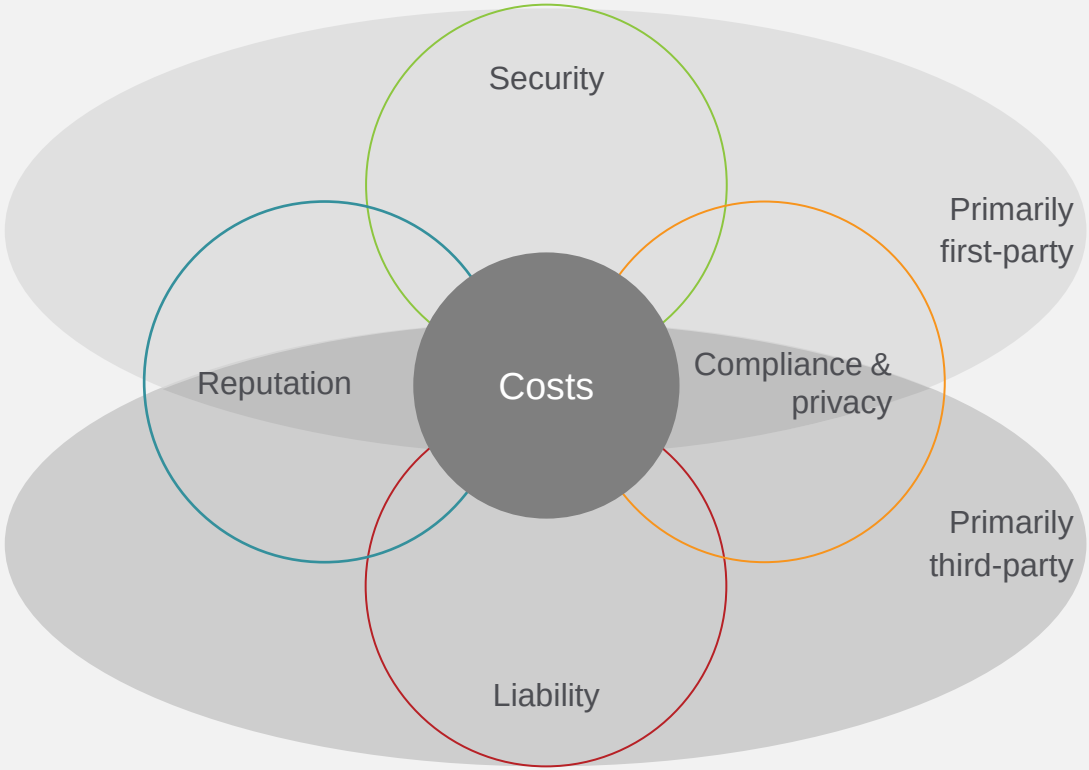


- **Identify**
  - Asset management, risk assessment, …
- **Protect**
  - Access control, awareness training, …
- **Detect**
  - Anomalies & events, security continuous monitoring, …
- **Respond**
  - Response planning, mitigation, …
- **Recover**
  - Recovery planning, improvements …
- Cyber insurance (powered by Munich Re)
- Risk gap
- Outage of external network exclusion

Icons: Munich Re

Dimensions of cyber risks

- Denial of service
- Extortion
- Electronic vandalism
- Theft of data
- Computer viruses



- Privacy laws
- EU directive
- HIPAA + HITECH
- Gramm-Leach-Bliley

- Loss of reputation after cyber incident
  - by third party
  - own fault
- Systematic posting of wrong information

- Intellectual property infringement
- Product/service failure
- Privacy violation

Introduction and Munich Re position in cyber

Munich RE

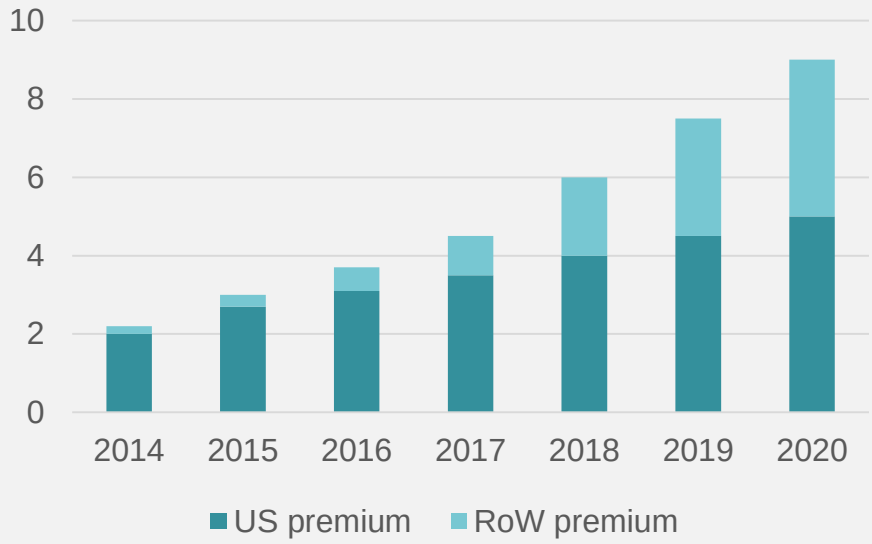
2

Image: used under license from shutterstock.com

Cyber (re)insurance market

Strong and long-term growth to be expected

GWP global cyber insurance market[1]



Driving forces/trends

- Digitalisation
- Global connectivity and interconnectedness; Internet of Things (IoT)
- Growth of virtual business models in many industries
- Rising legislation and internal governance requirements, as well as awareness of claims development
- New cyber products and extension of existing insurance coverages
- Large accumulation potential

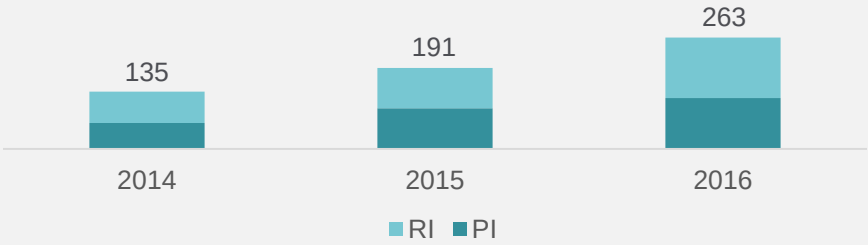
Munich Re will cautiously participate in the growth of this market segment.

1 Estimates based on different external sources (Marsh & McLennan, Barbican Insurance, Allianz).

Munich Re's cyber business strategy

Premium development Munich Re cyber portfolio

m$



- High investment into build-up of underwriting and risk management capabilities (e.g., technology knowledge, gathering of loss and exposure data, pricing, accumulation control, "dynamic" risk assessment)
- Collaboration with external partners in specific areas (e.g., risk assessment, data and modelling, claims management)
- Cautious deployment of single-risk and accumulation capacity, in line with growing expertise

Munich Re business units

Reinsurance

- Partnership with selected cedents
- Sharing of knowledge, methodologies and data

Hartford Steam Boiler (HSB)

- Cyber primary insurance covers for SME and individuals

Corporate Insurance Partner (CIP)

- Traditional and non-traditional cyber solutions for commercial and corporate enterprises

Munich Re will cautiously participate in the growth of this market segment.

Cyber – going into detail

Image: used under license from shutterstock.com

Wording

Munich RE

Image: Corbis

Munich Re modular wording

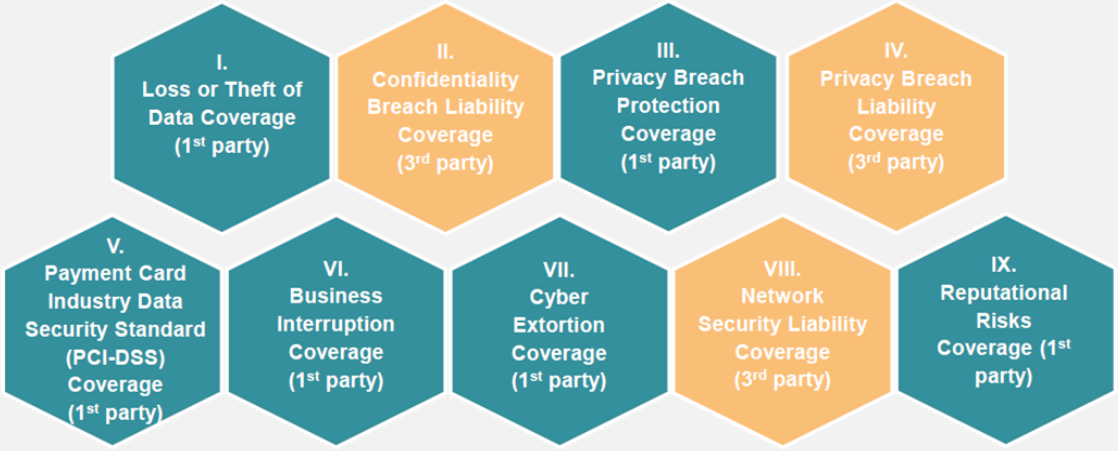
How it is structured

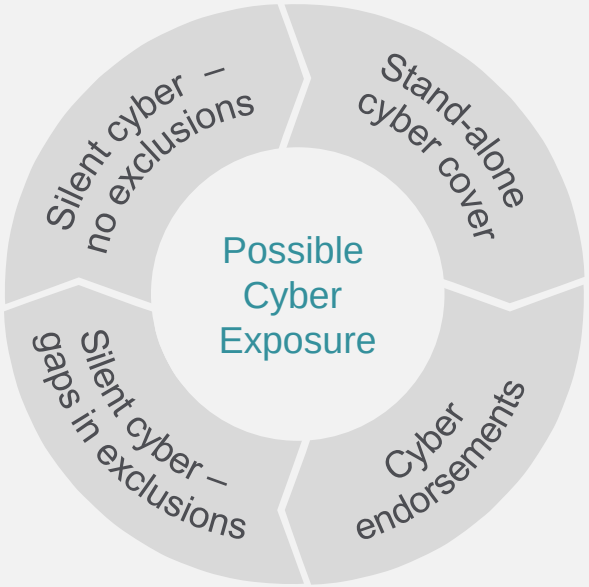
Munich RE

1	"Model" wording	To be adapted to ▪ the legal environment of the specific market ▪ the cedant's needs, e.g., type of insureds/activities the product is targeted for
2	Modular system	▪ Up to nine independent coverage sections ▪ To be assembled according to the cedant's needs
3	General target group	Applicable for small and medium-sized enterprises, as well as for larger risks

Potentially exposed insurance products

Munich Re cyber covers



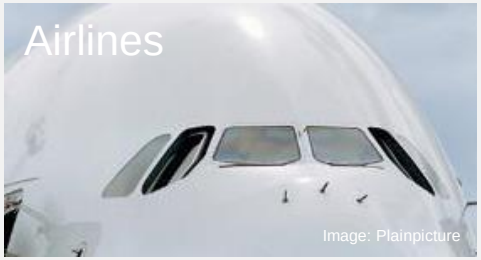


Property	Casualty	Marine	Agro	Health	Aviation	Life

Examples of silent cyber risk

Possible loss scenarios

Fourth industrial revolution?!



LOT grounding
June 2015
1,400 passengers

Dyn DDoS attack
Oct 2016
Amazon, Airbnb, BBC, PayPal, Visa

Jeep Cherokee
July 2015
AC, wipers, brakes!

Ukraine blackout
Dec 2015
225,000 customers

Risk assessment

Munich RE

Image: Corbis

The risk assessment

Structure of Munich Re cyber questionnaire: Medium and small version (1)

Company: General information: e.g. industry, activity, turnover, US exposure, IT & IT security budget

Insurance: Information about requested and prior insurance, limits and retentions

Data: Quality (= type, e.g. PII, PCI, PHI) and quantity (= volume, number of unique records).

Services: Outsourcing of IT services to third parties, risk assessment and contract design

IT Security: Organizational and technical criteria

History: Events, claims and losses

Assessment of cyber risks

Structure of Munich Re cyber questionnaire

The evaluation of the maturity of IT security assesses the covered exposure

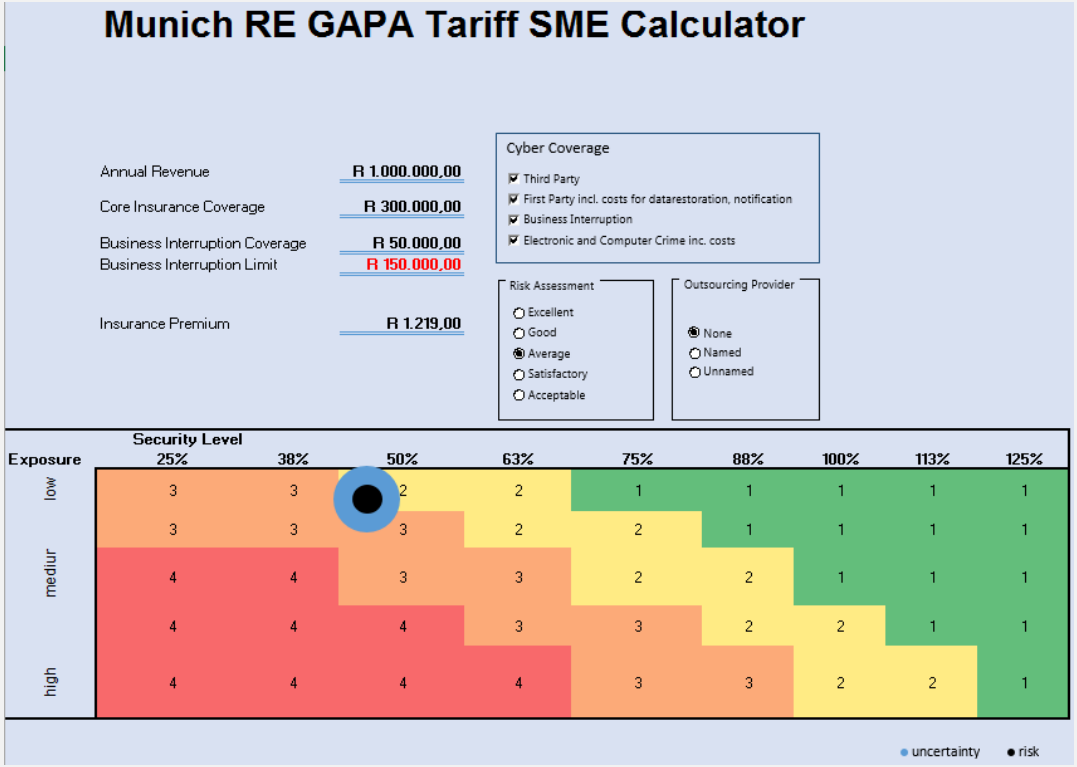
1. Organization
2. Information security governance and compliance
3. Inventory and classification of assets
4. IT system hardening and encryption
5. Patch management
6. Malware protection
7. Application security
8. Network security
9. Access control
10. Risk assessment, incident management, disaster recovery and business continuity
11. Awareness

Pricing

Munich RE

Image: Corbis

Pricing
Methodology (example)



Cyber accumulation

Munich RE

Image: Corbis

Cyber accumulation

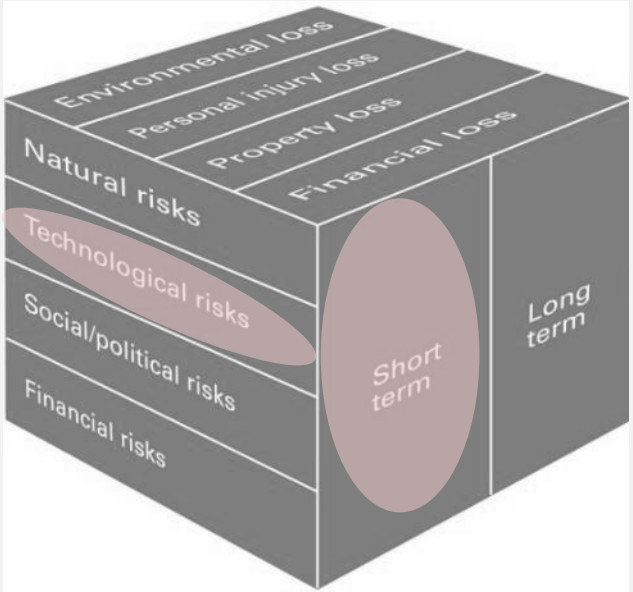
General remarks on cyber accumulation risk management

Objectives

- Identification of worst-case scenarios
- PML quantification and accumulation control
- Modeling of accumulation loss distributions in internal capital model

Overarching premises for cyber accumulations

- Assessment of generic PML scenarios with maximum loss potential for Munich Re
- Development of bottom-up and/or top-down approaches depending on underlying complexity and available statistical data



Cyber accumulation

General remarks on cyber accumulation risk management

Scenario	Self-reproducing Computer Viruses	Targeted cyber attack against critical infrastructure	Corrupted software in core module	Data Breach scenario affecting multiple insureds	Failure of IT service provider
Description	▪ Untargeted cyber attack on multiple computer systems ▪ Large number of systems infected by one event	▪ High loss potential ▪ Power outage, telecommunication network (Internet) outage	▪ Randomly falsified data over a longer period of time ▪ Data compromise across multiple clients & industries	▪ Criminal motivation: Financial gain by exploiting privacy data ▪ Many insureds affected (exploit of common vulnerability by hackers) ▪ Healthcare industry potential target	▪ Outage of cloud service provider ▪ Multiple cloud clients affected by Contingent/Business Interruption (CBI/BI) losses
Effect on cyber coverages	First party BI and data losses		First party BI and data losses	Privacy breach & cyber liability, cyber extortion	First party BI/CBI and data losses for non-physical damage triggers
Effect on standard P&C Lines of Business		Property & BI/CBI and liability losses	Professional liability (D&O, E&O) losses	Liability (PI, D&O, GL, MedMal) losses	First party BI/CBI losses for physical damage triggers
MR risk management	PML calculation model in place	Strict limitation or exclusion of first party exposures	Lower PML assessment as compared to other scenarios	Monitoring of exposed (cyber) participations	▪ Monitoring of limits for named service providers ▪ Low limits/exclusion for unnamed service providers
Accumulation potential for primary insurers	High in cyber insurance	High	For the time being low to medium	High in cyber insurance	Can be high for large cyber portfolios, expected to grow in future

Claims management

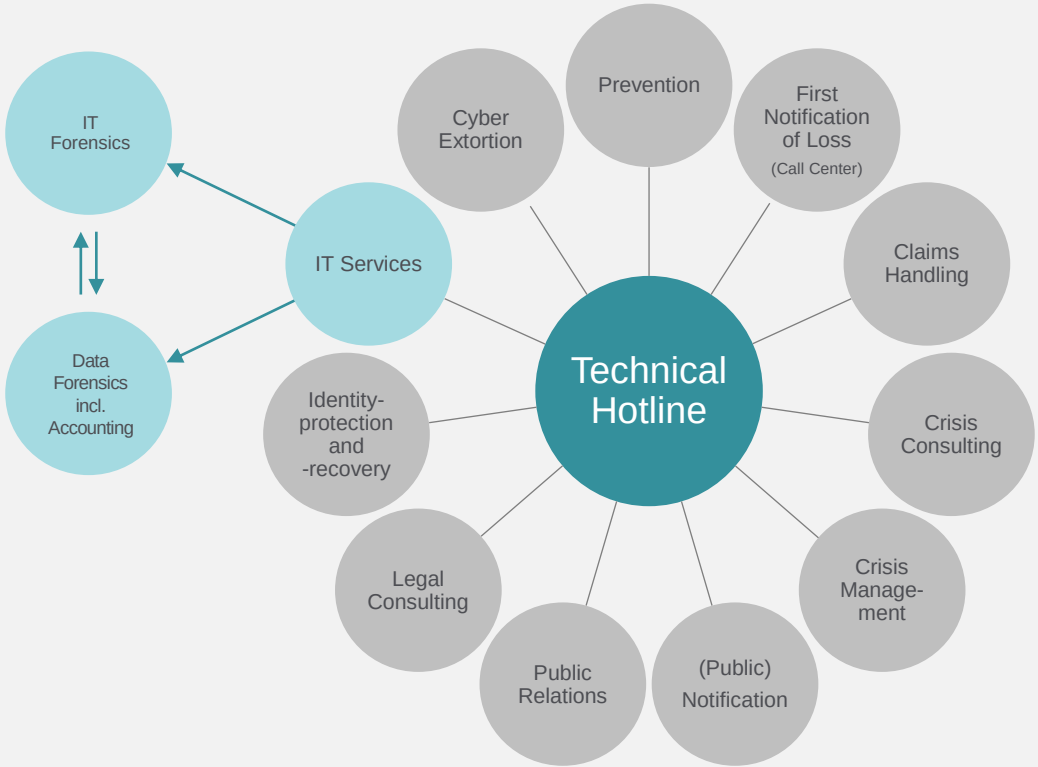
Munich RE

4

Image: used under license from shutterstock.com

Claims management

Service provider network



Munich Re services

Image: used under license from shutterstock.com

Your Munich Re services

Collaboration in the different steps of developing a cyber product

Thank you for your attention!

Carsten Topsch

Munich RE