19th HydraMeeting
20-22 September 2017

Jose Fidalgo,

Regional Head of Risk Consulting Liability

Central & Eastern Europe,

Allianz Global Corporate Specialty SE

(GERMANY)

HELLENIC ASSOCIATION OF INSURANCE COMPANIES

Thursday, 21.9.2017

Allianz Global Corporate & Specialty

Cyber Risks

Landscape, threats and impact…
what's new?

HYDRA Meeting, September 2017

Allianz

José Fidalgo

Regional Head of Risk Consulting Liability CEE

- Graduate Engineer
- Joined Allianz Global Corporate & Specialty in 2005
- Works in Business Line Liability as a Senior Risk Consultant
- Focus on Automotive, Electronics, ICT, FM and Chemistry
- Was before with Philips Electronics for 19 years

Expertise and Knowledge

- Six Sigma Black Belt
- ITIL
- Kéki R. Bhote alumnus "World Class Quality - Using DoE to make it happen“

Motto

"The formulation of a problem is the most essential part of problem solving"

© Copyright Allianz Global Corporate & Specialty 17-09-28

Agenda

1. The Situation Today
2. New Technical Requirements
3. Summary
4. Discussion

https://www.youtube.com/watch?v=lSbtpXMA3KE

http://www.youtube.com/watch?v=BcTU1GiluHg

© Copyright Allianz Global Corporate & Specialty 17-09-28

Digitalization is here to stay…

Where do we stand 2017

- Self-organizing supply chains
- Dependency from ICT increases
- Threat intelligence – anomaly detection

- Digitalization – Industry4.0
- Risk management requirements change
- Regulatory dito

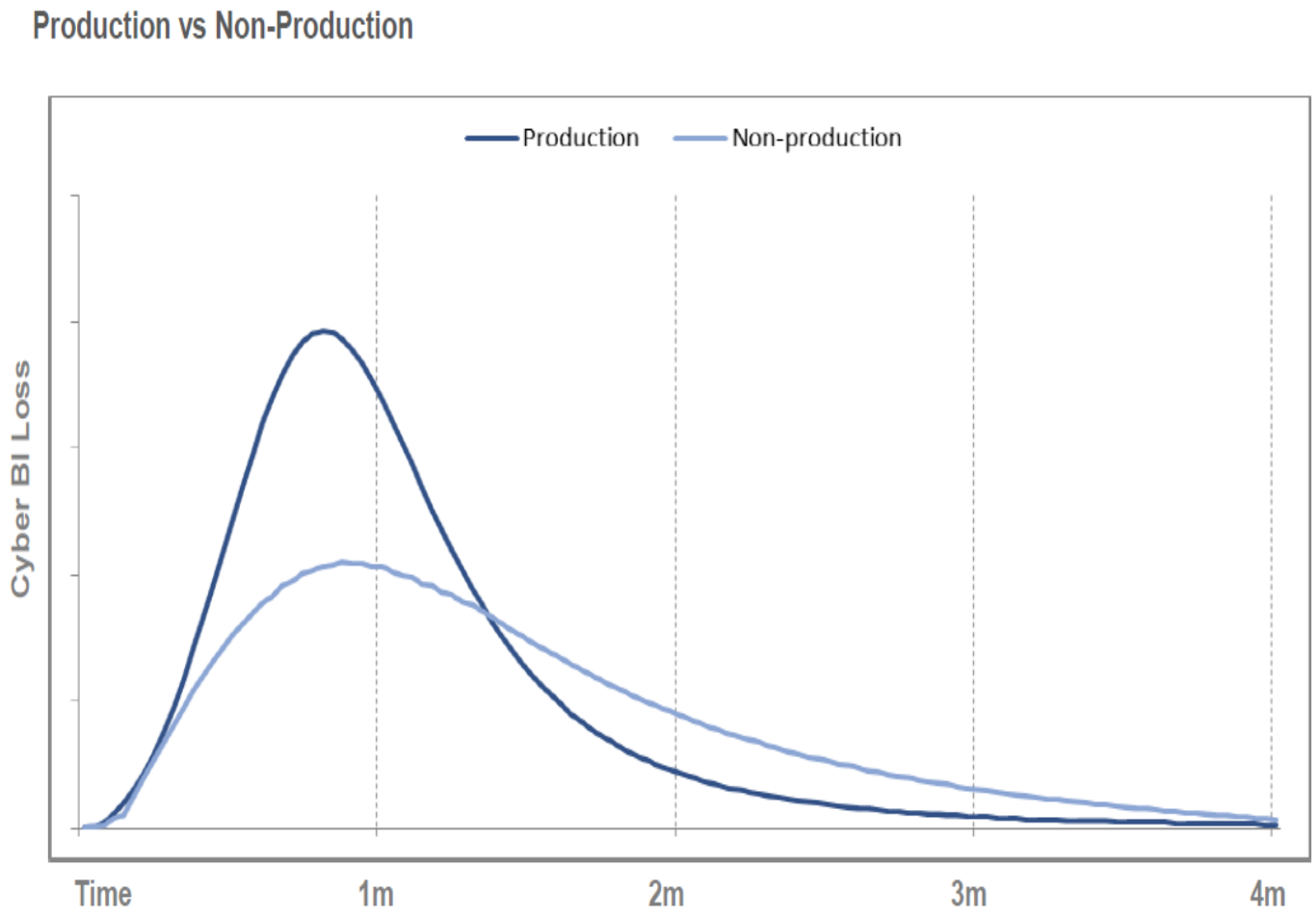
- Enterprise Resource Planning via Telematic and SCADA / ICS
- Application opportunities increase daily
- HBI: identification – protection – detection – response

- Outsourcing of IT-processes: “Cloud” **BUT:** responsibility for data and information still remains!
- Agile Processes are vital

- SMART products: SMART-Home
- Mobile Devices
- BIG DATA

© Copyright Allianz Global Corporate & Specialty 17-09-28

Cyber Business Interruption Development



© Copyright Allianz Global Corporate & Specialty 17-09-28

…and so are the risks!

© Copyright Allianz Global Corporate & Specialty 17-09-28

Risk management approach S.C.A.P.

The so called "*cyber risks*" have become part of the general business risks.
Therefore, threat modeling has become the crucial part of the preventive Risk Management **and** Business Continuity Management (BCM) process.

- **Safety/Security** and **Compliance** risks attract a lot of attention.
  The reasons are high visibility and significant effects, if a malfunction occurs in these categories.

- **Availability** risks are taken more and more seriously: even minimum deficits in this area can continue through the downstream value chain and generate big losses.

- In today's extremely networked world, managers understand that a wide spectrum of IT incidents affect operational sequences, **performance** and results of the enterprise.

(IT) risk management on the basis of SCAP categories is a never ending process!

© Copyright Allianz Global Corporate & Specialty 17-09-28

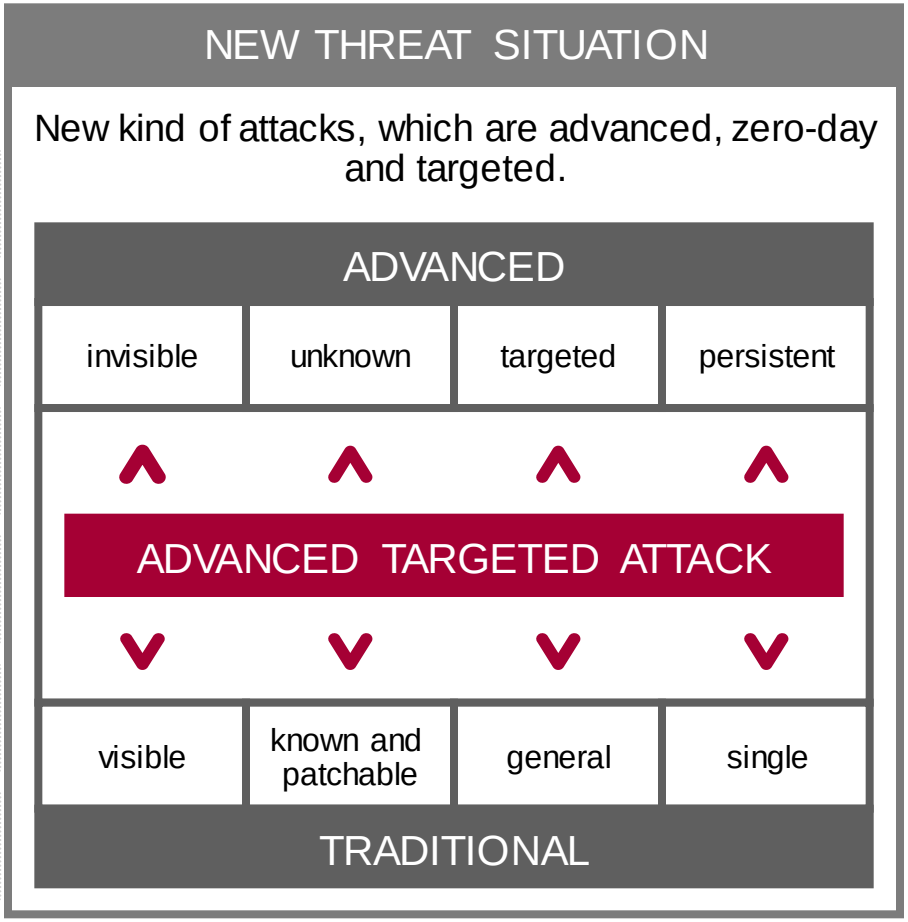
When threats come true… every company is a potential victim

Various computers of internal software developers were infected	Apple, SONY	100 million customer data records stolen PSN offline for one month
Attackers accessed computers in the editorial offices over an extended period	The Washington Post, belgacom	Highly-developed Trojan software found on PCs and servers
Data of 250,000 accounts stolen with passwords	twitter, LOCKHEED MARTIN	IT attack on the defense industry
Various computers of internal employees were infected with malware	facebook, Zappos.com POWERED by SERVICE	24 million customer data records stolen
Successful attack was announced, details not published	Microsoft, HBGary DETECT. DIAGNOSE. RESPOND.	Theft of internal and confidential customer documents (e.g., from the FBI and NSA)
Targeted attack on a defense group, details not published	EADS, LinkedIn	Theft of 6.5 million SHA1 password hashes
Over months, attackers accessed computers in NYT's editorial offices	The New York Times, last.fm	Theft of 2.5 million MD5 password hashes

© Copyright Allianz Global Corporate & Specialty 17-09-28

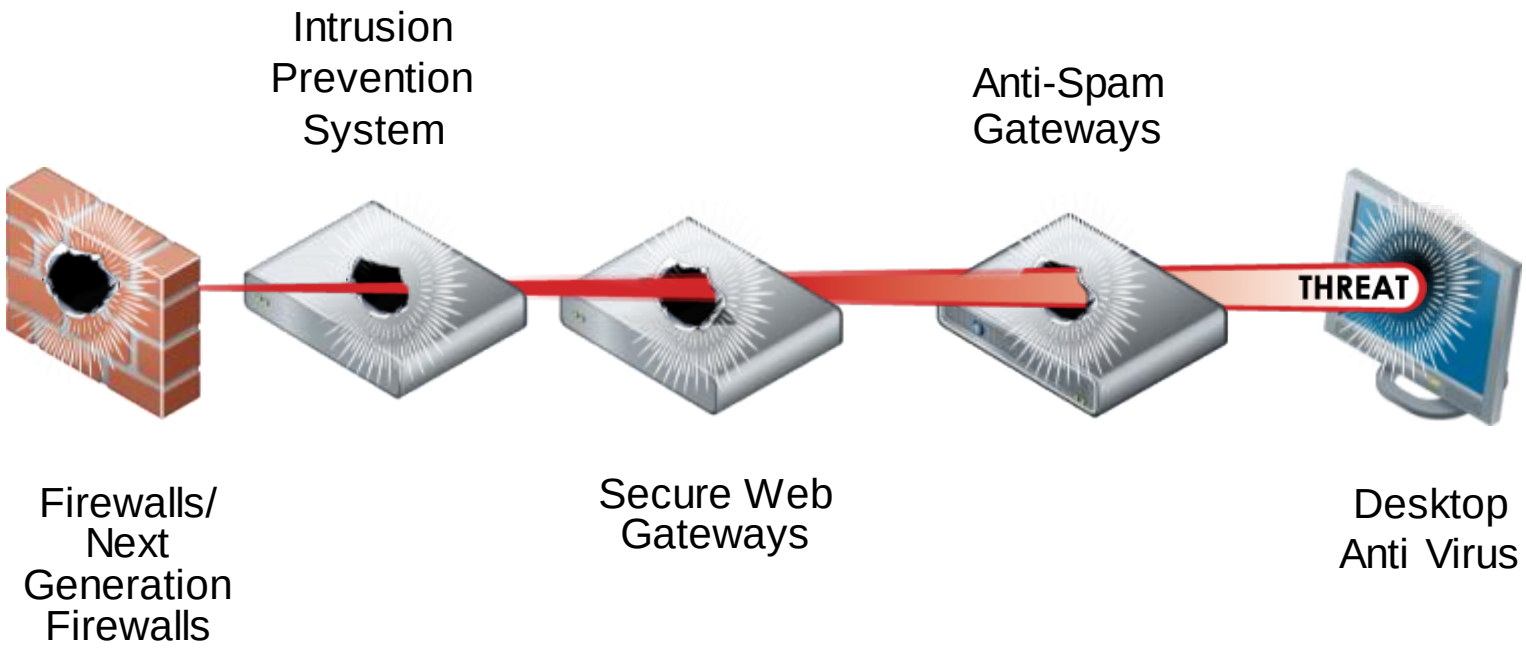
When threats come true… targeted attacks

- are using advanced techniques and/or malware
  - unknown
  - targeted
  - polymorph
  - dynamic
  - personalized
- are using zero-day exploits, commercially available toolkits and social engineering
- are often targeting intellectual property (espionage) and credentials (passwords)
- infiltrate the whole network (lateral movements)
- Also known as Advanced Persistent Threat (APT)



© Copyright Allianz Global Corporate & Specialty 17-09-28

When threats come true… traditional (technical) defence mechanisms do not work



© Copyright Allianz Global Corporate & Specialty 17-09-28

When threats come true… a cocktail of risk management and defence mechanisms works

Prevention of risks

Acceptance of risks

Risk - threat modelling and mapping

Control of risks

Mitigation of risks

Transfer of risks

Assessment of risks

Avoidance of risks

© Copyright Allianz Global Corporate & Specialty 17-09-28

When threats come true … Allianz Cyber Protect – risk transfer

Allianz Cyber Protect

Standard

- Standardised product with broad cover
- Easy application process
- Limit up to 10m EUR

Premium

- Extended Business Interruption cover
- Risk assessment with Allianz Risk Consulting
- Limit up to 100m EUR

Plus

- Tailor made solutions
- Full risk assessment with Allianz Risk Consulting and external partners
- Limit up to 100m EUR

© Copyright Allianz Global Corporate & Specialty 17-09-28

Allianz Cyber Protect: the solution in summary

- Three customized solutions
- Market leading capacity €100m
- Extended Business Interruption
- Forensic, crisis communications and legal experts instantly available
- Clear and consistent policy language
- A broad range of cyber exposures addressed in one policy family
- Simple application process for the standard cover

© Copyright Allianz Global Corporate & Specialty 17-09-28

Dimensions of Loss in a Cyber Incident

Third-party damage

- Breach of private data
- Breach of confidential corporate information
- Network Liability: Third party loss due to cyber attack against company
- Violation of rights via publications on digital media

First-party damage

- Business Interruption
- Additional costs (e.g. data reconstitution)
- Crime, IT theft
- Cyber extortion
- Notification Costs
- Legal costs
- Damaged Reputation: lost revenues

Regulatory

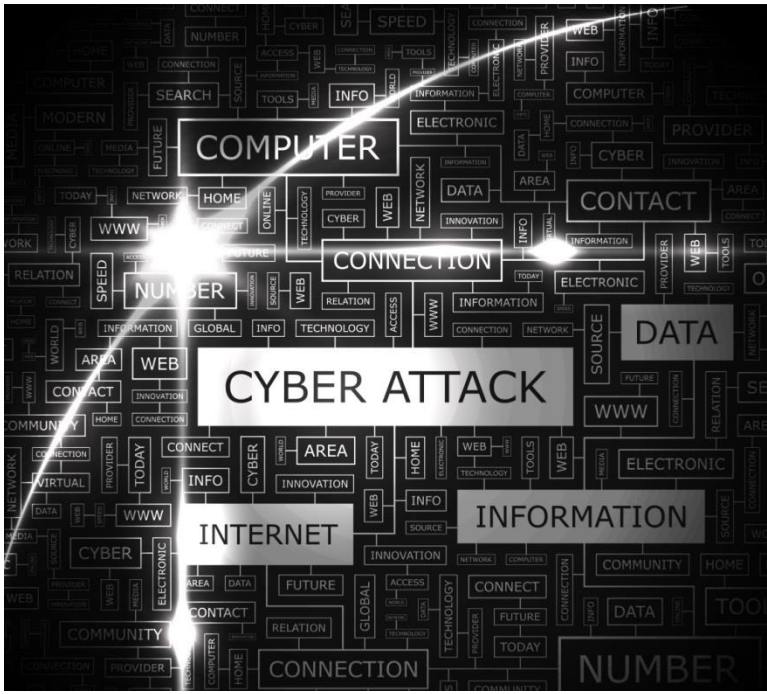
- Worldwide trend to extended notification requirements
- EU draft "General Data Protection Regulation" includes fines of up to 2% of annual global sales)
- Legal costs for regulatory proceedings

© Copyright Allianz Global Corporate & Specialty 17-09-28

1. Is there a need for Cyber Insurance?

?

“Are our Cyber exposures adequately addressed under our existing insurance programs?”



© Copyright Allianz Global Corporate & Specialty 17-09-28

Is there a need for Cyber Insurance?

Existing traditional covers are not designed to specifically respond to cyber exposures

- Notification Costs?
- Forensic Costs?
- Regulatory proceedings / Fines?
- Non-damage BI?
- Data recovery?

Solution: Specific cross line "**one-stop-shop cover**" for different Cyber risks as an "umbrella".

© Copyright Allianz Global Corporate & Specialty 17-09-28

Allianz Cyber Protect (overview)

Offering cover for the broad scale of cyber risks

Allianz Cyber Protect

- Data breach liability
- Data breach costs (notification costs etc)
- Network security claims
- Media liability
- Regulatory Investigations: defence costs + fines & penalties (where legally permitted)
- E-Payment (Payment Card Industry): Contractual Penalties / fraude due to misuse of Payment Card

- Business interruption and extra expenses due to Cyber Attack
- **BI "Premium"**: due to technical failure and human error
- **BI "Premium Plus"**: CBI (Contingent Business Interruption)
- Data reconstitution costs
- Cyber crime – transfer of funds
- Cyber extortion
- Crisis communication
- IT Consultant Services

© Copyright Allianz Global Corporate & Specialty 17-09-28

Case example

Scenario description

- Due to a hacker attack into the computer system of company Alpha 3.000.000 sets of personal client data including credit card data are stolen. Clients in European and non-European countries (including US) are affected.
- Several data protection regulators in US and Europe are investigating the incident.
- Claim on behalf of an affected client (class action) and by the credit card provider.
- Sales of Alpha drops significantly.
- Securities class action against company and management alleging insufficient disclosure. Shareholder derivative claim against board members alleging lack of risk management.

© Copyright Allianz Global Corporate & Specialty 17-09-28

Case example

Exposure	Allianz Cyber Protect
▪ Privacy breach claims of clients	▪ Privacy Breach cover: damages + defence costs
▪ Credit card provider claims, contractual penalties	▪ Network security claims cover + E-Payment cover for penalties and misuse of Credit Card, exchange of Credit Cards, Credit Monitoring, etc.
▪ Forensic Costs	▪ IT Consultant cost cover
▪ Notification Costs	▪ Response cost cover
▪ Regulatory proceedings	▪ Regulatory cover: legal costs + fines (if permitted)
▪ Drop of sales	▪ Crisis Communication Cover

Shareholder class action and shareholder derivative claims: **D&O**

© Copyright Allianz Global Corporate & Specialty 17-09-28

The Cyber Market

USA

- Start in the early 1990ties
- 30 + carriers
- Capacities of 600 Mil. + available
- Very well developed marked – companies do buy cover
- More than 2.5 Bil. US$ premium income, growth rate 20%+

Europe

- Started in 2010
- 20 + carriers
- Capacities of 500 Mil. + available
- Market is in its infancy - Companies need to be convinced

© Copyright Allianz Global Corporate & Specialty 17-09-28

Insurance Cyber Survey
The Process

Phase 1	Phase 2	Phase 3	Phase 4	Phase 5
Desktop analysis	Interviews	HQ Meeting	Operational sites	Workshops
▪ Pre-insurer reports ▪ Broker tendering ▪ Web presence	▪ Questionnaire to be filled out in advance of meeting ▪ Assessment	▪ Risk Management: SCAP structure ▪ Assessment ▪ Management control system ▪ Core IT process	▪ IT checklist ▪ Assessment	▪ IT risk workshops on a regular basis

In more than 50% of our assessments, we identify weak or poor (IT) processes in companies.

© Copyright Allianz Global Corporate & Specialty 17-09-28

AGCS IT Maturity Model
The Levels 1 to 3

The **AGCS IT Maturity Model** consists of 6 levels, ranging from status „red“ (very low standard / insufficient) to „green“ (very high standard / good). Each level is defined via different characteristics. This model is another tool for AGCS experts to assess the IT risks of a company.

Level	Characteristics of Level	Status
1	▪ **No PM*:** insufficient, incomplete, no process structure ▪ No process or described. The (process) result is not defined.	
2	▪ **Non R & R**:** deficient performed process decomposition ▪ Single process steps are carried out. Steps are not defined and vary unplanned. The process performs the desired results, but without repeatability and reproducibility.	
3	▪ **Try & Error:** sufficiently managed, but uncontrolled body of process landscape ▪ Process sequences defined and in use, workflows exist. But no coordination! No overall awareness of processes being the base. Changes are the result of "try & error"	

* Process management

**Repeatability and Reproducibility

© Copyright AGSE SE

© Copyright Allianz Global Corporate & Specialty 17-09-28

AGCS IT Maturity Model

The Levels 4 to 6

Level	Characteristics of Level	Status
4	▪ **MCRS*:** satisfactory / good, established managed approved, controlled body of process landscape ▪ The processes are based on planned, structured and documented descriptions. The processes are coordinated, roles and responsibilities are well-regulated. Structure with measuring criteria for success and performance (KPIs) is implemented.	■ □ □
5	▪ **BSC**:** good / very good, predictable process results ▪ For established processes exist regularly measured quality targets. Based on these targets, process improvements are possible. Process results are predictable. Controlled output with good quality (workflow).	■ □ □
6	▪ **Kaizen**: very good / excellent, permanent Deming Cycle ▪ There is a planned continuous improvement process coordination with the development of business objectives. Processes are analyzed with SWOT criteria. CSF and OFP for each process are transparent. High flexibility due to continuous PDCA process .	■ □ □

* Management Control and Reporting System

**Balanced Scorecard

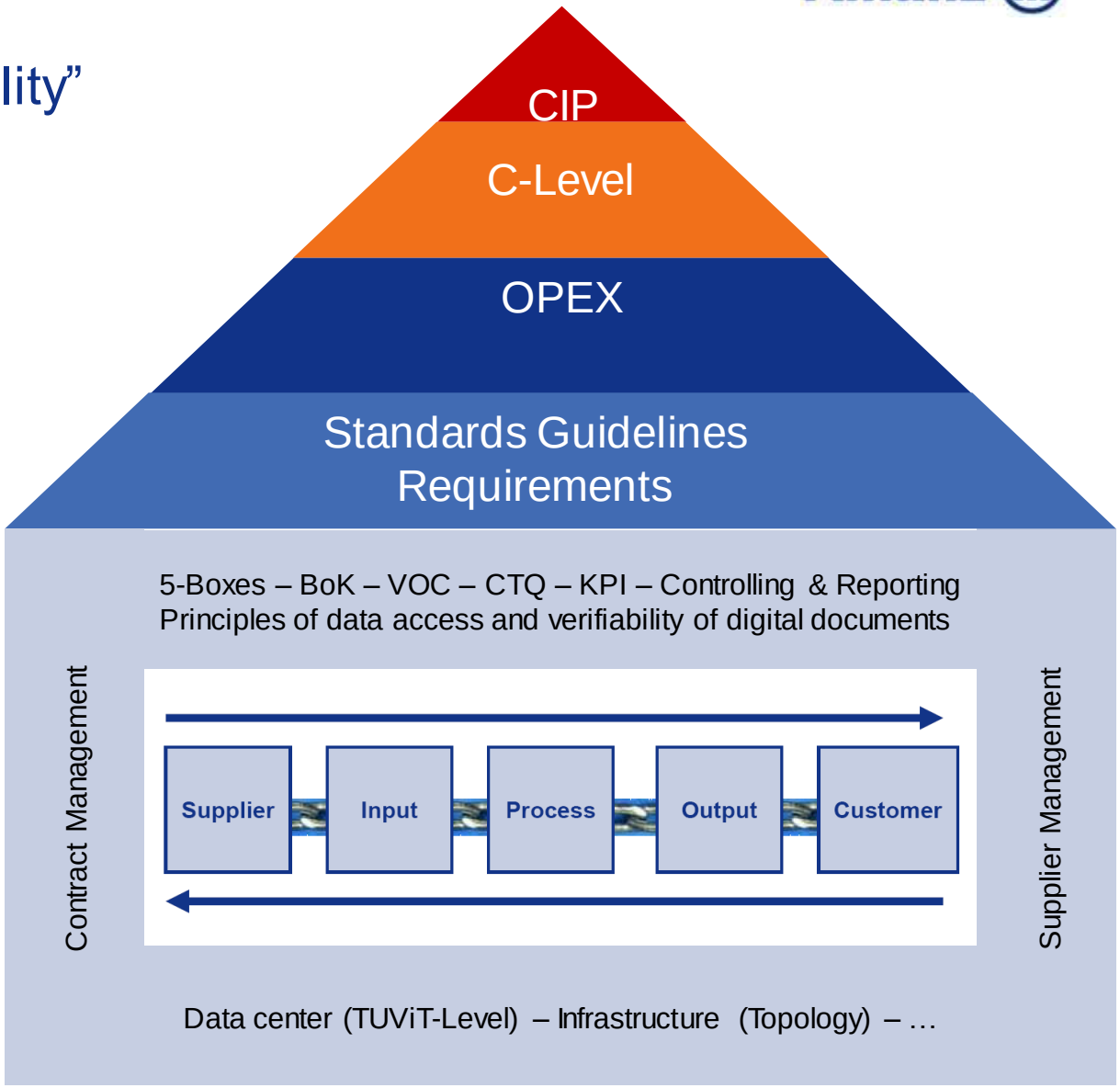
© Copyright AGSE SE

© Copyright Allianz Global Corporate & Specialty 17-09-28

“The House of IT Quality”

The concept

- AGCS developed a tool for the transparent measuring and evaluation of a company's IT environment.
- IT-infrastructure forms the basis, followed by business processes and industrial standards at the top.
- “*The House of IT Quality*” is a comprehensive approach, which delivers all facts that need to be taken into consideration regarding the appropriate insurance cover for IT risks.

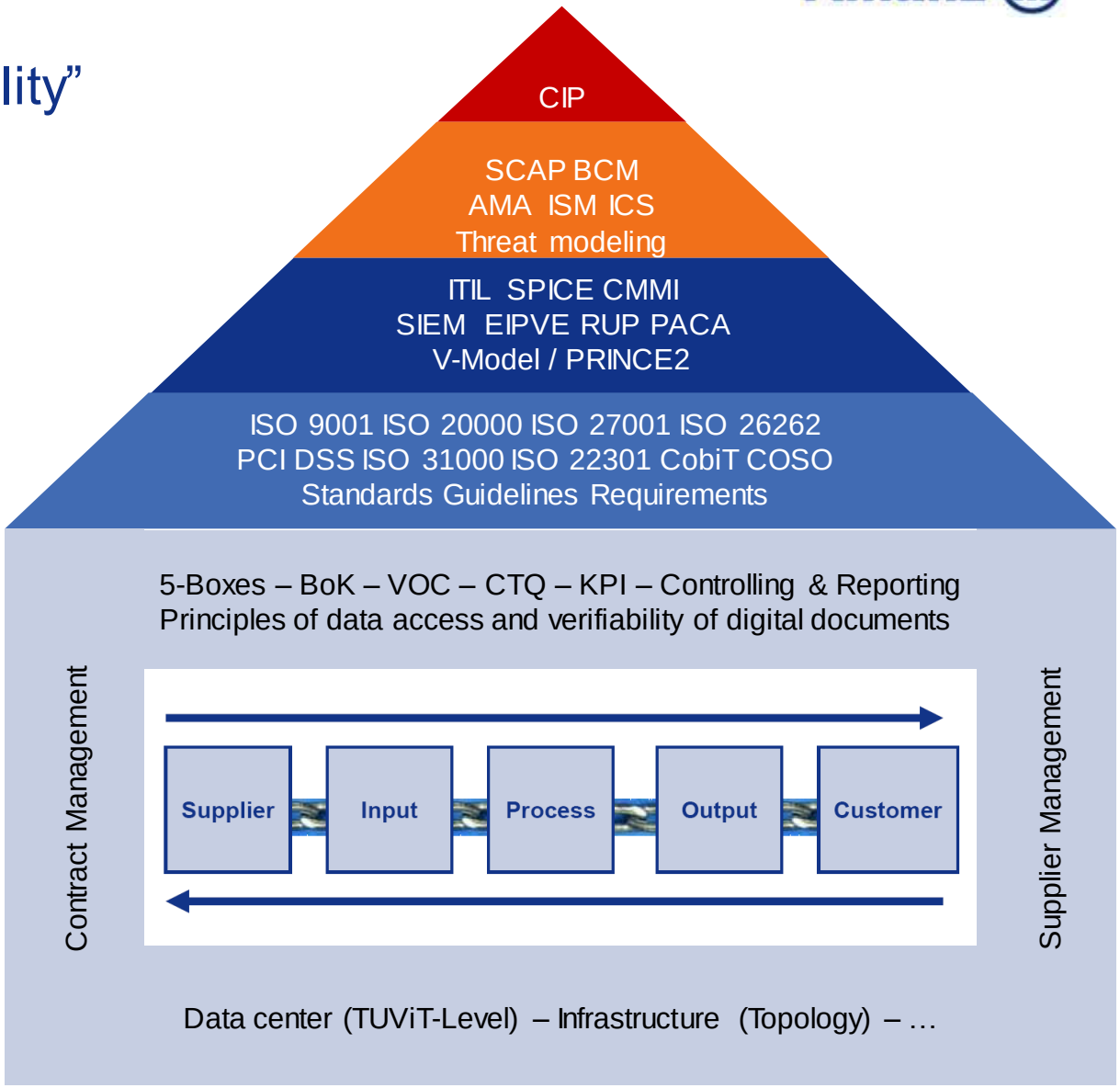


© Copyright Allianz Global Corporate & Specialty 17-09-28

“The House of IT Quality”

The concept

- AGCS developed a tool for the transparent measuring and evaluation of a company's IT environment.
- IT-infrastructure forms the basis, followed by business processes and industrial standards at the top.
- “*The House of IT Quality*” is a comprehensive approach, which delivers all facts that need to be taken into consideration regarding the appropriate insurance cover for IT risks.



© Copyright Allianz Global Corporate & Specialty 17-09-28

The AGCS IT Risk Model
Categories

Risk Category 1

- Internal web pages and / or internet presence (creation, maintenance)
- E-Mails (technical transaction)
- Technical operation of electronic data exchange via e-mail and www

Risk Category 2

- Hardware / parts of hardware (manufacturing, sales, distribution etc.)
- Access providing
- Content providing for external websites
- E-Commerce
- Call Center Management

Risk Category 3

- Software (development, sales & distribution, consultation, etc.)
- Consulting regarding products and services within the IT sector

Risk Category 4

- IT networks
- Electronic data processing (external data)
- Operational control of IT infrastructure for external clients (outsourcing)
- Cloud Computing
- Remote maintenance or remote control
- Industrial IT

© Copyright AGSE SE
© Copyright Allianz Global Corporate & Specialty 17-09-28

Joint Workshop Concept Overview

Interactive, Business-oriented and result-driven

START

Get a clear and common understanding about the impact of cyber risks from a technology and insurance perspective

IDENTIFICATION OF BUSINESS-RELATED THREAT AREAS

Analyze threat situation based on customer business model.
Define and map relevant threat scenarios

PRIORITIZATION OF ACTION FIELDS

Classify and point out threat scenarios against risk management measure taken so far

EVALUATE CUSTOMER SITUATION

Analyze selected threat scenarios/action fields and identify first solutions to improve security level

EXPERT FEEDBACK

First view on customer situation from a joint T-Systems/Allianz perspective.
Recommend appropriate assessment and solutions

NEXT STEPS

Agree on follow-up and a rough roadmap to increase security maturity level

NEXT LEVEL

© Copyright Allianz Global Corporate & Specialty 17-09-28

Joint Workshop Concept

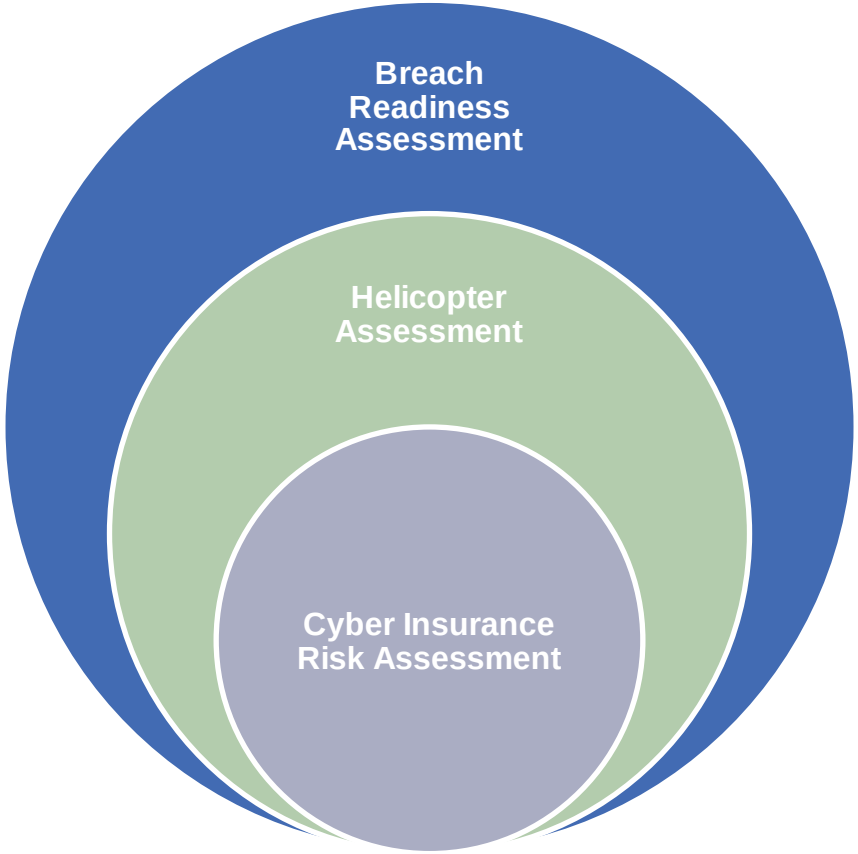
Clients benefit and outcome

360° Risk Management	• Introduction to holistic risk management: technology, organization and insurance
Systematic appraisal of the risk situation	• Structured dialogue with all stakeholders to identify threat situation and areas of action
Basis for decision	• Creation of a reliable decision-making basis for further action
Measures / solutions	• Demonstration of coordinated risk management measures

© Copyright Allianz Global Corporate & Specialty 17-09-28

Assessments formats

All assessments include the insurance risk assessment ("insurability of cyber risks")



Breach Readiness Assessment

The Advanced Cyber Defense (ACD) Breach Readiness Assessment provides a comprehensive view of an organization's current state and its ability to respond to any potential threats or security incidents.

Duration: 5 weeks

Helicopter Assessment

Comprehensive Assessment of the cyber risk maturity level of a focus area, for example, incident coverage skills, customer data protection, etc. The assessment includes aspects of technology and control processes as well as the insurance-related analysis of a probable maximum loss (PML).

Duration: 1 Week

LIFE IS FOR SHARING.

Cyber Insurance Risk Assessment

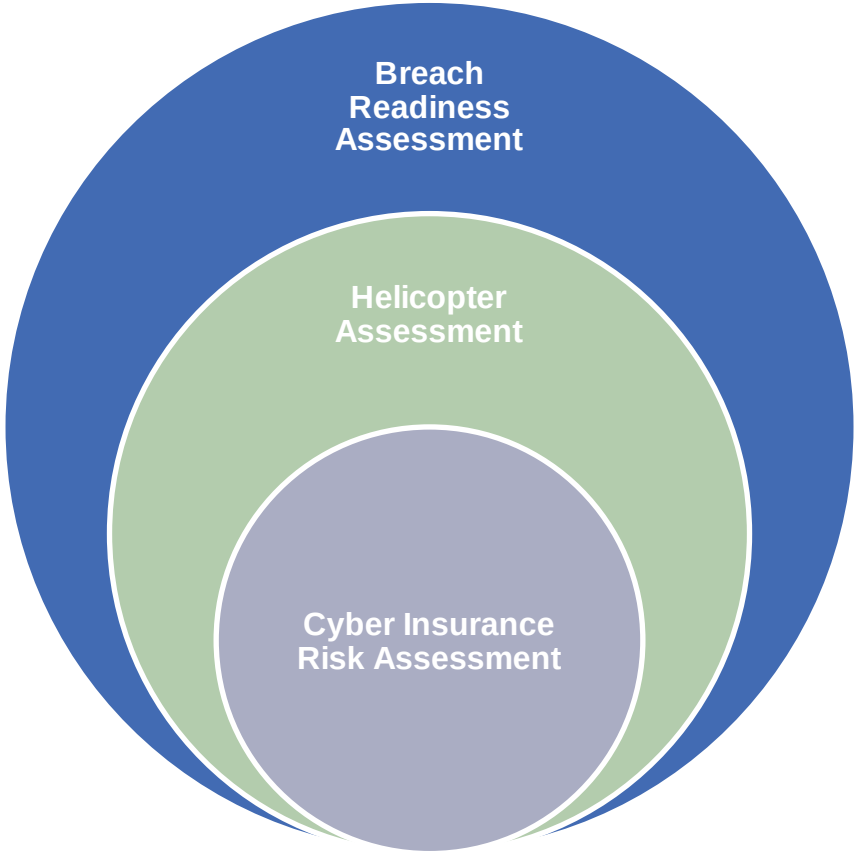
Requirement for an insurance quote. High-level assessment of the cyber risk maturity level according to the Capability Maturity Model, including industrial IT and maximum probable loss (PML).

Duration: 1 day (Risk Assessment)

© Copyright Allianz Global Corporate & Specialty 17-09-28

Joint assessments

All assessments include the insurance risk assessment ("insurability of cyber risks")



Value added

Insurance Quick Wins

Technology Quick Wins

© Copyright Allianz Global Corporate & Specialty 17-09-28

Our Principle

Not the certificate, but the **performance of a system** must be the goal.

© Copyright Allianz Global Corporate & Specialty 17-09-28

Summary
"Body of Knowledge" in Information Security

- ☑ **Awareness campaign in ICT**: value chain – infrastructures - dependencies; DIE or you DIE
- ☑ **Risk management**: threat modelling
- ☑ **HBI**: Identification – protection – detection – response
- ☑ **Threat intelligence**: anomaly detection (APT)
- ☑ **Security**: vulnerability management; BYOD – UYOD
- ☑ **Industrial IT**: SCADA & Industrial 4.0; self-organizing sup-cha
- ☑ **Megatrends**: Big Data; Mobility; Cloud Computing

© Copyright Allianz Global Corporate & Specialty 17-09-28

Summary and potential for improvement

“Threats (1-5) for Industrial Control Systems (ICS)”

Source: Bundesamt für Sicherheit in der Informationstechnik

- ☑ **unauthorized use of remote maintenance access**
- ☑ **online-Attacks via office- / enterprise-Network**
- ☑ **attack against inserted Standard-Components in the ICS- Network**
- ☑ **(Distributed) Denial-of-Service-Attacks**
- ☑ **human malpractice/error and act of sabotage**

© Copyright Allianz Global Corporate & Specialty 17-09-28

Summary and potential for improvement

“Threats (6-10) for Industrial Control Systems (ICS)”

Source: Bundesamt für Sicherheit in der Informationstechnik

- ☑ **Injection of malicious codes via external hardware**
- ☑ **Reading and writing messages in the ICS network**
- ☑ **unauthorized access to resources**
- ☑ **Attacks on network components**
- ☑ **technical misconduct and force majeure**

© Copyright Allianz Global Corporate & Specialty 17-09-28

Lets discuss!

- ☑ **Massive increase of cyber attacs**
- ☑ **Attacks are well planned and successful**
- ☑ **Traditional defense mechanisms do not work**
- ☑ **Threat modelling – threat matrix – mapping**
- ☑ **Classic Hacker – org crime – hacktivists – intelligence services**
- ☑ **Joint assessments**
- ☑ **…**

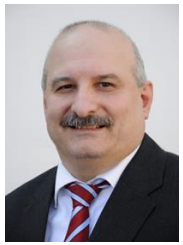
© Copyright Allianz Global Corporate & Specialty 17-09-28

More questions?
Contact Details

Jens Krickhahn

Regional Practice Leader
Financial Lines CEE
Cyber, Fidelity & PI
Jens.krickhahn@allianz.com

+49 711 2173-3751



José Fidalgo

Regional Head of Risk
Consulting Liability CEE

Jose.fidalgo@allianz.com

+49 89 3800-13204

Visit us online at
www.agcs.allianz.com

© Copyright Allianz Global Corporate & Specialty 17-09-28

Allianz Global Corporate & Specialty

Thank you for your attention.

José Fidalgo

AGCS SE