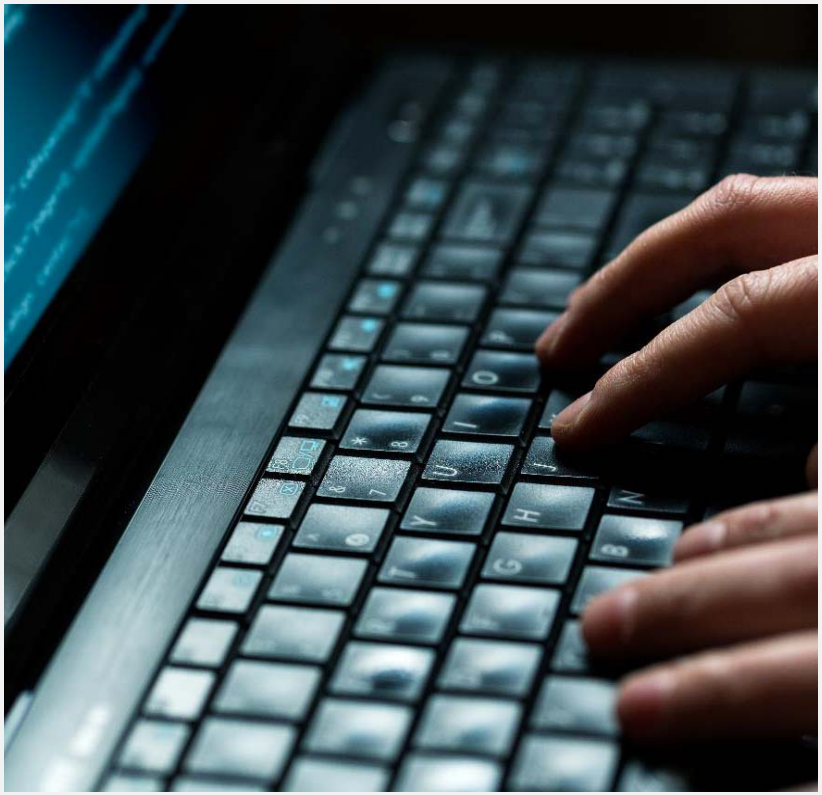
# Cyber Risks - Engineering Insurers Perspective

**MIA Working Group Paper 98 (16)**
**IMIA Annual Conference 2016 - Doha, Qatar**
October 4, 2016

Alexander Schmidl – Munich RE

# OVERVIEW

- What is it all about?
- Objectives
- IMIA Workgroup
- Scope & Content
- Some Highlights
- Q&A



# WHAT IS IT ALL* ABOUT?
# *CYBER RISK IN ENGINEERING LINES

**Physical damage** caused by cyber

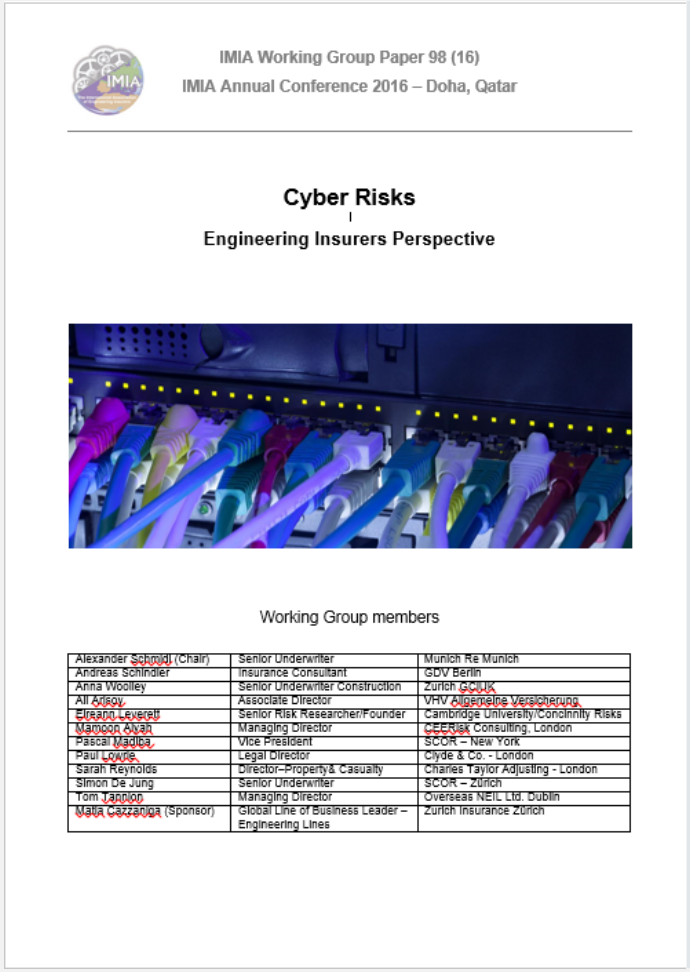
Silent Engineering **All Risks Policies cover** cyber peril

Physical damage **losses are paid by insurers**

**Lack of Cyber underwriting** and **premium** calculation

Cyber Risk in Engineering **more complex** than asumed

# OBJECTIVES OF THE CYBER WORKGROUP



IMIA Working Group Paper 98 (16)
IMIA Annual Conference 2016 – Doha, Qatar

**Cyber Risks**

**Engineering Insurers Perspective**



Working Group members

| | | |
|---|---|---|
| Alexander Schmidl (Chair) | Senior Underwriter | Munich Re Munich |
| Andreas Schindler | Insurance Consultant | GDV Berlin |
| Anna Woolley | Senior Underwriter Construction | Zurich GCUK |
| Ali Arbov | Associate Director | VHV Allgemeine Versicherung |
| Eireann Leverett | Senior Risk Researcher/Founder | Cambridge University/Concinnity Risks |
| Mamoon Alyan | Managing Director | CEERisk Consulting, London |
| Pascal Madiba | Vice President | SCOR – New York |
| Paul Lowne | Legal Director | Clyde & Co. - London |
| Sarah Reynolds | Director–Property& Casualty | Charles Taylor Adjusting - London |
| Simon De Jung | Senior Underwriter | SCOR – Zürich |
| Tom Tannion | Managing Director | Overseas NEIL Ltd. Dublin |
| Malta Cazzaniga (Sponsor) | Global Line of Business Leader – Engineering Lines | Zurich Insurance Zürich |

to publish a paper in October 2016:

- dedicated to engineering underwriters and risk managers
- increasing their awareness for cyber risks in engineering lines
- providing practical underwriting guidance and claims considerations

# IMIA CYBER RISK WORKING GROUP

## Working Group Members

| | | |
|---|---|---|
| **Alexander Schmidl (Chair)** | Senior Underwriter | Munich Re Munich |
| **Anna Woolley** | Senior Underwriter Construction | Zurich GCiUK |
| **Ali Arisoy** | Associate Director | VHV Allgemeine Versicherung |
| **Eireann Leverett** | Senior Risk Researcher/Founder | Cambridge University/Concinnity Risks |
| **Mamoon Alyah** | Managing Director | CEERisk Consulting, London |
| **Pascal Madiba** | Vice President | SCOR – New York |
| **Paul Lowrie** | Legal Director | Clyde & Co. - London |
| **Sarah Reynolds** | Director–Property& Casualty | Charles Taylor Adjusting - London |
| **Simon De Jung** | Senior Underwriter | SCOR – Zürich |
| **Tom Tannion** | Managing Director | Overseas NEIL Ltd. Dublin |
| **Matia Cazzaniga (Sponsor)** | Global Line of Business Leader – Engineering Lines | Zurich Insurance Zürich |

# SCOPE & CONTENT

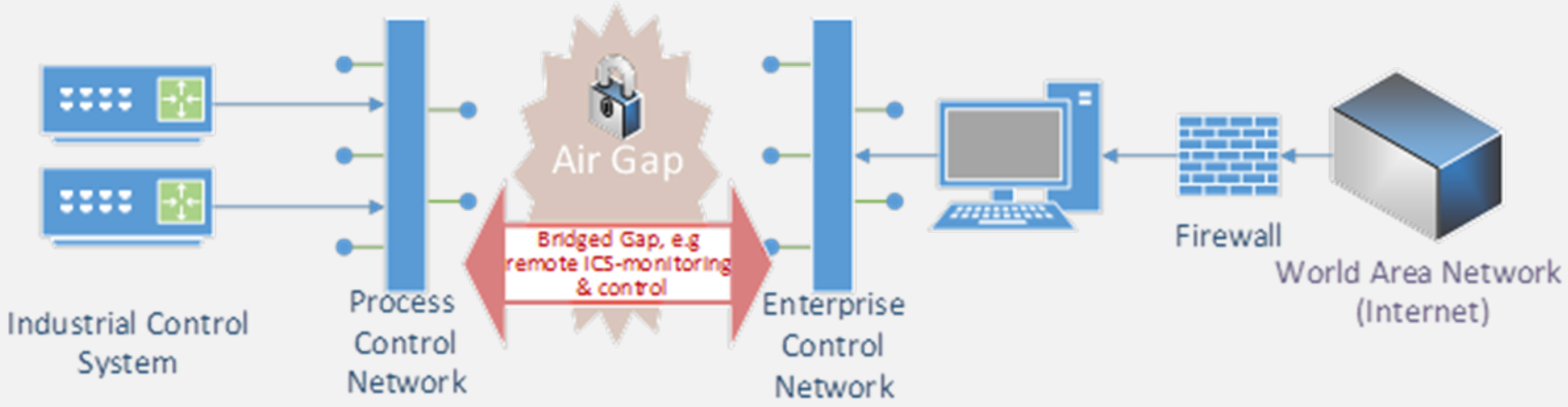
# SCOPE & CONTENT

# SOME HIGHLIGHTS
# 1- Underwriting Decision Options iro Cyber Risk

| Like it (Price it) | Leave it (Exclude it) | Change it (Limit it) |
|---|---|---|
| Provide Cyber cover either via:<br>• Standalone Cyber Policy or<br>• Exclusion (see 5.3.3) and Write-back endorsement (see 5.3.4) or<br>• Under unchanged "All risk" engineering policies, assessing and pricing cyber risk. Refer to section 5.-Underwriting Considerations | Use advanced exclusion clauses (See section 5.3.3) and accept the effort of proving cyber root causation in origin, (i.e. without in-depth investigation). | Mitigate the risk by<br>• Inserting obligations in the wording referring to agreed standards regarding risk compliance, security and safety with the insured (refer to risk assessment standards, section 5.1)<br>• Change the risk profile through interfacing with the general risk and compliance team. |
| **Pro´s:**<br>• Monetizing market demands<br>• Risk partnering with insured<br>• Adequate risk return | **Pro´s:**<br>• Minimizing risk in the engineering book of business<br>• Potential for adequate risk return | **Pro´s:**<br>• Business can be retained |
| **Con´s**:<br>• Difficult to sell in overcapitalized markets<br>• Adequate cyber pricing is challenging due to lack of historical data, metrics and models | **Con´s:**<br>• Difficult to enforce<br>• not a useful risk solution for the insured<br>• remaining risk not monetized | **Con´s:**<br>• Difficult to enforce<br>• Still not charging premium for exposure.<br>• Potentially not meeting clients expectations |

# SOME HIGHLIGHTS
## 2 – Threats from Industrial Control Systems (ICS) 1/3

ICS were designed for reliability and continuous operation of industrial processes. The fundamental design was performed before communication networking was usual i.e. formerly existing air gaps between Internet and ICS are often bridged




ICS so are accessible from the www, if administrator login credentials get “phished” Patches and updates to ICS are very seldom (only during maintenance, with manufacturer´s permission), vulnerabilities can be exploited

# SOME HIGHLIGHTS
# 2 – Threats from Industrial Control Systems (ICS) 2/3

## EXAMPLES OF INCIDENTS

Das Kernkraftwerk Gundremmingen soll 2021 abgeschaltet werden.
(Foto: KGG)

Dienstag, 26. April 2016

**Alarm in Gundremmingen**

**Computervirus in Kernkraftwerk entdeckt**

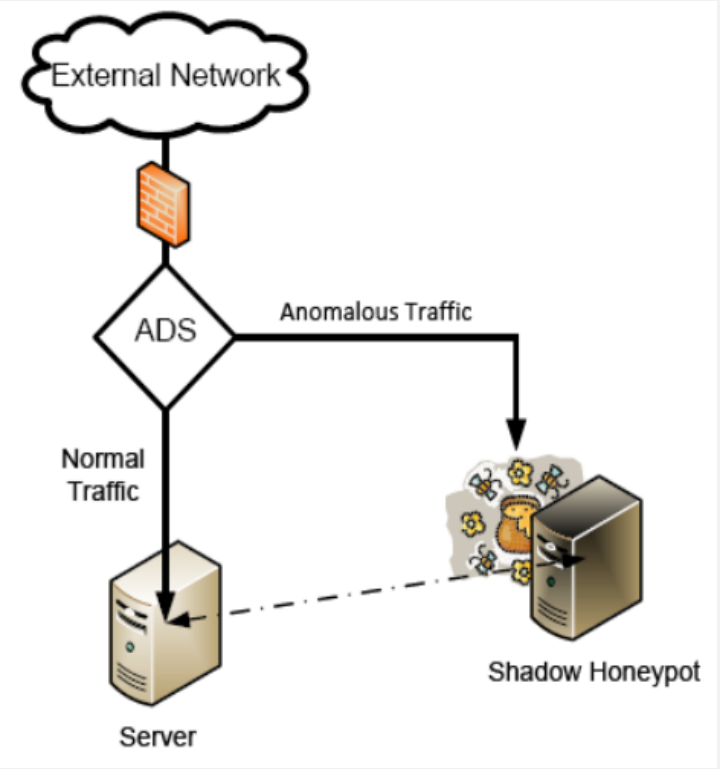
**Im Kernkraftwekt Gundremmingen wird bei Routinekontrollen auf einem Computer der Steuerungsanlage für Brennelemente ein Virus entdeckt. Der Betreiber stuft den Vorfall als "normal" ein, die Sicherheit des Kraftwerks sei nie gefährdet gewesen.**

### Bavarian Nuclear PP:

Malicious code discovered in the fuel handling machine of Gundremmingen NPP :

- Possible infection via USB Stick discarded
- Investigations by german BSI agency revealed: virus introduced at equipment manufacturer. No harm due to airgap between machine and www.

# SOME HIGHLIGHTS
# 2 – Threats from Industrial Control Systems (ICS) 3/3




**Honeypot -** German **“**TÜV Süd“ attracts hackers

For test purposes TÜV certification agency installed a virtual sewage plant in the www and attracted hackers. „During the **8 months** lasting test phase we registered **more than 60 000 unauthorized accesses** from all parts of the world, primarily from Asia and US", says TÜV-Rep Axel Stepken and further comments:

- IP-Adresses are not always an indication of the origin of the attacks – many of those use anonymized IP-adresses
- Attacks are not not only performed by criminals but also by „white“ hackers

http://www.sueddeutsche.de/wirtschaft/virtuelles-wasserwerk-tuev-sued-lockt-hacker-an-1.2947371

# SOME HIGHLIGHTS
# 3- Discussion of Engineering Cyber losses 1/2

## 4.5 EXAMPLES OF INCIDENTS AND LOSSES IN ENGINEERING LINES

### 4.5.1 LOSSES FROM OPERATIONAL RISKS

2014 GERMAN STEEL MILL - (PD/BI - LOSS)

2015 UKRAINIAN POWER GRID BLACKOUT - (BI - LOSS)

2008 TRAM DERAILMENT IN LODZ, POLAND - (PD - LOSS)

2005 DAIMLER-CHRYSLER - (PD/BI – LOSS)

2001-2002 MAROOCHYSHIRE – (PD – LOSS)

### 4.5.2 LOSSES FROM PROJECT RISKS

2011 CONCENTRATED SOLAR POWER PLANT IN UAE (PD-LOSS)

More incidents see: http://www.risidata.com/Database/event_date/desc

# SOME HIGHLIGHTS
## 3- Discussion of Engineering Cyber losses 2/2

2014 GERMAN STEEL MILL - (PD/BI - LOSS)

https://www.youtube.com/watch?v=OVMwI2TWrZw

| | |
|---|---|
| **Cyber scenario:** | Targeted malicious attack |
| **Method:** | Access to the enterprise´s office network via a Spear Phishing Mail. By gathering admin login credentials further access to the industrial process network. |
| **Loss Effect:** | Massive Ethernet traffic on the proces network leading to failure of control components, inhibiting a controled shutdown of a furnace, finally leading to a € 20m from ground up physical damage and business interruption loss |
| **Claim:** | under property reinsurance treaty |
| **Attacker´s profile**: | expert knowledge. The compromise involved many different IT systems including industrial control systems. |

# SOME HIGHLIGHTS
# 4 – Advanced Cyber Exclusion and Write-Back Endorsements

## Endorsement – Advanced Cyber Exclusion 2016 (Draft)

Notwithstanding any provision to the contrary within this Policy or any endorsement thereto, it is understood and agreed as follows:

1. Any loss, damage, liability, costs or expenses directly or indirectly caused by or contributed to or resulting from the following shall be excluded from indemnification and are not covered by this Policy, regardless of any other cause or event contributing concurrently or in any other sequence to the loss, damage, liability, costs or expenses:

   a) **Damage to or Loss of Data** occurring on the **Insured's Computer Systems**, or

   b) a **Computer Malicious Act** on the **Insured's Computer Systems**, or

   c) **Computer Malware** on the **Insured's Computer Systems**, or

   d) a **Cyber Extortion**.

2. Where this Cyber Exclusion is endorsed on Policies covering risks of war or terrorism this Cyber Exclusion shall only exclude **Cyber Terrorism** or **Cyber War** according to **Clause 1** above.

3. The Insurer is only obliged to indemnify the Insured in accordance with this Policy if the Insured fully complies with the following cumulative conditions:

3.1 While this Policy is in effect, the Insurer or an **Expert**, agent or a representative of the Insurer may, at any reasonable time, inspect and examine the Insured's premises, the Insured Property, the **Insured's Computer Systems**, and the Insured's **Computer Networks** in order to conduct claims handling. The Insured shall in a timely manner provide the Insurer or an **Expert**, agent or a representative of the **Insurer** with all relevant details and information that may be required by the **Insurer** for its claims handling. Additionally, the **Insured** shall ensure that the **Insurer** or an **Expert**, agent or a representative of the **Insurer** is allowed to inspect any **Outsourcing Provider** of the Insured if such an inspection is required to conduct claims handling.

3.2 Upon the occurrence of any loss event that might give rise to a claim under this Policy, the Insured shall

3.1.1 cooperate at all times with the Insurer or an **Expert**, agent or a representative of the Insurer with regard to the loss event that might give rise to a claim under this Policy;

3.1.2 do and permit to be done anything that may be practicable to support the Insurer or an **Expert**, agent or a representative of the Insurer in order to establish the cause and extent of the loss or damage resulting from the loss event that might give rise to a claim under this Policy;

3.1.3 preserve any hardware, software and **Data** which may be affected by the loss event that might give rise to a claim under this Policy and make them available for inspection by the Insurer or an **Expert**, agent or a representative of the Insurer as long as required by them;

3.1.4 furnish any information, reports, materials, **Data** and documentation that the **Insurer** or an **Expert**, agent or a representative of the Insurer may require; and

3.1.5 support the Insurer or an **Expert**, agent or a representative of the Insurer in any forensic investigation of the cause of any loss event that might give rise to a claim under this Policy and in any preparation of the documentation of the results,

4. The boldfaced, capitalized terms used in this Cyber Exclusion Endorsement shall have the following meanings:

**Computer Malicious Act**
Means any wrongful act carried out through the use of **Data**, **Computer Systems** or **Computer Networks** with the intention to cause harm. The term **Computer Malicious Act** shall also encompass a **Denial of Service Attack**.

**Computer Malware**
Means any hostile or intrusive software, including computer viruses, spyware, computer worms, trojan horses, rootkits, ransomware, keyloggers, dialers, spyware, adware, malicious browser helper objects and rogue security software, designed to infiltrate and disrupt computer operations, gather sensitive information, or gain access to **Computer Systems** without consent.

**Computer Network**
Means a group of **Computer Systems** and other computing hardware devices connected via a form of communications technology, allowing the networked computing devices to exchange **Data** and other resources, along **Data** connections, including the internet, intranet and virtual private networks (VPN).

**Computer Systems**
Means the IT, industrial process control and communications systems as well as any other item or element of hardware and IT infrastructure, software or equipment that is or may be used for the purpose of creating, accessing, processing, protecting, monitoring, storing, retrieving, displaying or transmitting **Data**.

**Cyber Extortion**
means any unlawful and intentional use of a threat or series of threats by an extortionist against the **Data** on an **Insured's Computer Systems** or against the **Insured's Computer Systems** in order to extract a **Cyber Extortion Ransom** from the Insured by use of coercion.

**Cyber Extortion Ransom**
means any sum of money, in cash or otherwise, funds or property, as well as goods, products and/or services that the Insured is forced to pay or hands to the extortionist.

**Cyber Terrorism**
Means any act or series of acts or threat thereof of any person or group of persons, whether acting alone or on behalf of or in connection with any organization through the use of **Computer Systems**, to destruct, disrupt, subvert or make use of any **Computer System**, **Computer Network**, IT infrastructure, the internet, the intranet, telecommunications and/or its content, with the intention to cause harm and committed for religious, ideological or political purposes including but not limited to the influencing of any government and/or to put the public or a section of the public in fear.

**Cyber War**
Means any state of hostile conflict (whether declared or not) to resolve a matter of dispute between two or more states or nations through the use of **Computer Systems** and via the internet, to destruct, disrupt, subvert or make use of any **Computer System**, **Computer Network**, IT infrastructure, the internet, the intranet, telecommunications and/or its content, with the intention to cause harm.

**Damage to or Loss of Data**
Means any introduction, corruption, creation, modification, alteration or deletion of **Data** which, when processed by a **Computer System**, may lead to an impaired, corrupted or abnormal functioning of the **Computer Systems** and/or the interruption or disruption of processing operations.

**Data**
Means any readable information, irrespective of the way it is used or rendered (text, figures, voice or images), including software or programs, transmitted or stored in a digital format outside the random access memory. For the avoidance of doubts the term **Data** shall not be considered Insured Property.

**Denial of Service Attack**
Means any malicious attack leading to a total or partial deprivation, disruption and/or unavailability of **Computer Systems** and network facilities being altered or destructed, by deluging and thus overloading **Computer Systems** with an incoming stream of requests, including distributed denial of service attacks, in which a multitude of compromised systems are used to coordinate a simultaneous attack.

**Employee**
Means any natural person that performs services or provides labour in the service and on the premises of the **Insured** under an express or implied employment contract, under which the Insured has the right to control the details of work performance. The term "**Employee**" shall also include external staff hired by the Insured in order to provide IT services working within the operational structure and under the functional authority of the Insured.

**Expert**
Means any person with a high degree of skill in or knowledge of a certain subject, including but not limited to IT specialists, lawyers, consultants or auditors.

**Insured's Computer Systems**
Means (i) the **Computer Systems** under the control and management of the Insured that are owned, licensed or hired by the Insured or (ii) any **Computer Systems** under the control and management of the **Outsourcing Provider** that are owned, licensed or hired by the **Outsourcing Provider** or the Insured or (iii) any **Computer Systems** under the control and management of a customer or supplier of the Insured that are owned, licensed or hired by the customer or supplier of the Insured.

**Outsourcing Provider**
Means any IT service provider that is assigned by the Insured by written contract to offer functions or services of management, maintenance and/or development for the benefit of the Insured on a **Computer System** that is controlled and managed by the IT service provider.

# SOME HIGHLIGHTS
## 4 – Advanced Cyber Exclusion and Write-Back Endorsements

NMA 2914,15,12 CL 380 not sufficiently exclude all instances of physical damage caused by cyber- incidents and there is lack of definition.

The **IMIA WORKGROUP ADVANCED CYBER EXCLUSION CLAUSE** applies to any (including physical) loss or damage directly or indirectly caused by or resulting from one or more of the following:

1) Damage to or Loss of Data occurring on the Insured's Computer Systems,
2) a Computer Malicious Act on the Insured's Computer Systems,
3) Computer Malware on the Insured's Computer Systems,
4) a Cyber Extortion.

Definitions are provided in the exclusion. Unlike CL380, no need for insurers to demonstrate an intention to cause harm on the part of the hacker.

Effective exclusion for the German steel-mill case, where it is believed that the physical damage was an inadvertent result of the hacker's activities.

# SOME HIGHLIGHTS
## 4 – Advanced Cyber Exclusion and Write-Back Endorsements

Note:

- The burden of proof for applying an exclusion is on the insurer

  and for that

- successful investigation about cyber as root cause is key

Therefore, the **IMIA WORKGROUP ADVANCED CYBER EXCLUSION CLAUSE** makes payment of any claim, not just a 'cyber claim', subject to a condition precedent regarding preservation of data and access to the assured's computer systems.

This should ensure that insurers' experts are given access to relevant computer systems where a cyber-attack is suspected, allowing an accurate and timely assessment of whether the loss has been caused by a cyber-attack.

# SOME HIGHLIGHTS
## 4 – Advanced Cyber Exclusion and Write-Back Endorsements

### IMIA WORKGROUP WRITEBACK ENDORSEMENT 2016 ALTERNATIVE 1 (DRAFT)

Issued to:

Issued by:

Effective:

Endorsement No.:

Subject to the terms, conditions, deductibles, limits, exclusions and extensions contained in this Policy, this Cyber Write Back Endorsement obliges the insurer to indemnify the Insured for any loss, damage, liability or expense which the Insurer would have been able to decline solely due to the operation of Clause 1. and/or Clause 2. of the Advanced Cyber Exclusion 2016 as agreed hereon by endorsement.

# SOME HIGHLIGHTS
# 5 – Success Factors in Claims Management

- Think about Cyber as possible cause for claimed physical damage
- Occurrence of PD within the policy period!, time of infection is not relevant
- Timeframes are important to secure evidence of cyber root cause, logs, screenshots witness statements help, particularly in view of a relatively long incubation period (average incubation period is 8 months)
- Clear instructions for claims management whether to involve loss adjuster or claims service provider
- Clear policy conditions particularly regarding exclusions and writeback will support loss adjustment. Clarity regarding insured perils, insured interests and insured objects is paramount. Unambiguous definitions are required for terms such as cyber incident, data, property damage, loss and occurrence.
  See also the definitions provided in the Advanced Cyber Exclusion Endorsement

# SOME HIGHLIGHTS
## 6 – Balance of Interests between Insurance Need and -Solution

An Insured would not like to find cyber excluded from his All Risks policy at renewal.

Likewise, a technical insurer would rightly be uncomfortable including silent and unknown cyber exposures (and worse still, including such cover without collecting an adequate additional premium for the exposures).

How can the dilemma be solved?

Do you know it?

# Q&A

- ? ?
- ? ?
- ? ? ?

THANK YOU!

IMIA
The International Association of Engineering Insurers