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 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

Rev. A002 16.9.2016

CONTENTS

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors of the IMIA workgroup, unless stated otherwise. This publication does not necessarily represent state-of-the-art and IMIA may update it from time to time.

Third-party sources are quoted as appropriate. IMIA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither IMIA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorized provided the source is acknowledged.

Version	***Author***	***Reviewed***	***Date***	***Status***	***Amendments***
Draft	*IMIA WGP - AS*	*Sponsor*	*24.05.2016*	*accepted*	*Final Draft reviewed by sponsor*
A001	*IMIA WGP – AS*	*Sponsor*	*22.08-2016*	*accepted*	*Clauses extracted to PDF file attachments*
A002	*IMIA WGP - AS*	*Sec.*	*16.09.2016*	*accepted*	*Reviewed Advanced Cyber Exclusion Clause- Appendix 5 & 6*

1 EXECUTIVE SUMMARY

"Cyber" is a generic term which can mean different things to different people. For clarity, this paper defines cyber risks and how they apply to Engineering insurance lines. Much is already known about cyber risk as it relates to electronic data, therefore this paper concentrates on the possibility of physical damage and consequential losses such as business interruption arising from a cyber event.

Cyber risk is real. Threat sources and the motivations for initiating a cyber-incident are manifold. They range from inadvertent and accidental incidents to theft of data, attempted extortion and the efforts of 'hacktivists' or 'state-sponsored' endeavours. Motivation is always expensive and sometimes impossible to prove. When evaluating cyber exposure with the intention of creating a potential stand-alone Engineering insurance product, or thinking about including cover by endorsement, or even if intending to impose an outright exclusion on a policy, the following key outputs from the workgroup´s analysis should be considered:

- Cyber threats have the potential to impact all businesses.
- Cyber exposures within Engineering and Specialty lines insurance are much more complex than is assumed and are generally underestimated by our industry.
- Engineering underwriters must address the issue of cyber on all covers they write.
- Engineering insurers have already paid out on policies for relatively inexpensive physical damage initiated by a cyber event. Forensic investigation of cyber as a 'root cause' analysis can be expensive and there may have been no initial reason to suspect anything untoward.
- Any Engineering lines policy that is silent on the matter of cyber should consider that damage is covered.
- Adopting a clear cyber exclusion is one way to help bringing some degree of certainty to all parties and it can also be used as the basis for creating a clear 'bolt-on' coverage or stand-alone product.
- Reliance on war- and terrorism exclusions may be ineffective if the root cause of any damage claimed cannot be accurately determined.
- For those underwriters interested in embracing some form of cyber add-on or inclusion or stand-alone Engineering cover, the following should be considered regarding project and operational risks:
    - threat factors to assess (e.g. vulnerabilities, exploits, Industrial Control Systems (ICS) - and cyber-physical-security threat actors, attack types and -stages) within and outside of ICS environments
    - key exposures to consider including, but not limited to
        - threat- and scenario analysis, exposure, complexity, IT security and maturity
        - aggregate exposure stemming from risk accumulation
        - wording considerations in order to limit an insured loss
    - a possible pricing approach to consider adopting or modifying
    - claims management considerations for different underwriting approaches
- As general statements or observations: The bigger the organization, the more difficult it is to secure from a cyber perspective. The more global the Engineering lines cover, the more susceptible it is to paying for physical and other damage that may have been cyber-initiated.
- Cyber threats are evolving and are continuing to evolve. Static security measures become quickly outdated.

Dependence on Information- and Communications technology (ICT) grows every year, and so does its vulnerability with regard to cyber threats.
Consequently this paper seeks to be of practical use for Engineering insurance lines underwriters. The recommendations provided are just that, recommendations. Insurance market considerations are

not part of this paper and individual underwriters should determine their own risk appetite and approach to this exposure.

2 INTRODUCTION

This paper should be of interest to Engineering and technical insurance line underwriters, risk managers, risk engineers, claims managers and brokers who have a desire to increase awareness of the rapidly evolving phenomenon known as “cyber risk” and its underwriting and claims implications.

In this paper 'cyber risk' is defined as:

"Risks arising from the storage, use, computation, and/or transmission of electronic data. Such cyber risks may be malicious, for example caused by individual hackers or nation states, or inadvertent, for example caused by a coding error."

Traditionally, in Engineering lines, cyber risk has been perceived as causing only non-physical damage 'harm' arising from data theft or corruption of data in Information Technology (IT) environments. Evidence shows, however, that physical damage as a result of cyber risk is not only possible but has already occurred. Such physical damage events, including consequential damages such as delay in start-up or operational business interruption, are a core focus of this paper. The paper discusses a variety of ways in which cyber risks impact those writing insurance for Engineering lines, either explicitly as 'cyber cover' or silently as part of an all-risks cover without (effective) exclusions. Put simply, cyber risk is an issue for all lines of (Engineering) insurance.

With a minimum technical IT background information and jargon, the paper focuses on potentially underestimated exposures stemming from related vulnerabilities and threat scenarios. The paper will illustrate possible impacts on different types of policies and analyze occurred incidents and loss examples. From these, underwriting and claims considerations are derived as a practical guide.

As technology and interconnectivity are dynamically evolving, factors like The Cloud, Shadow IT, Mobile and flexible working, Bring your own, and Internet of Things (IoT) are also influencing the threat landscape for Engineering risks. More detail is provided in section 7.

Keeping pace with trends is key if Engineering underwriters are to remain current in assessing and carrying risk. Continuous learning will qualify insurers to be long-term risk partners for the industry and its increasingly complex risks.

3 A DECISION IS NEEDED

Cyber is a root cause with consequences. It may or may not result in physical damage. When an insurance policy is silent there are consequences. The assumption must be that if a policy is silent, cover will attach. In a similar manner, the role and effectiveness of exclusions needs to be considered carefully.

How and when can an insurer rely on such exclusions? What level of effort/cost is required to satisfy the successful application of an exclusion? Such considerations apply regardless of whether you are looking at an "all risks" or standalone cyber policy.

In the vernacular, the options for Engineering underwriters are: "Like it, Leave it, or Change it".

Like it (Price it)	Leave it (Exclude it)	Change it (Limit it)
Provide Cyber cover either via: • Standalone Cyber Policy (under any line of business) or • Exclusion (see 5.3.3) and Write-back endorsement (see 5.3.4) or • 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 • 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) • Change the risk profile through interfacing with the general risk and compliance team.
Pro´s: • Monetizing market demands • Risk partnering with insured • Adequate risk return	**Pro´s:** • Minimizing risk in the Engineering book of business • Potential for adequate risk return	**Pro´s:** • Business can be retained
Con´s: • Adequate cyber pricing is challenging due to lack of historical data, metrics and models	**Con´s:** • Difficult to enforce • not a useful risk solution for the insured • remaining risk not monetized	**Con´s:** • Difficult to enforce • Still not charging premium for exposure. • Potentially not meeting clients expectations

Table 3.1 Ways to deal with cyber exposure in Engineering lines

If underwriters choose to affirmatively write cyber covers in Engineering lines of business (the "Like-it" approach above), or want to increase awareness of exposures (the "Change it" approach), the following section provides insights, thoughts, facts and examples regarding Cyber Risk in Engineering business.

4 CYBER RISK IN ENGINEERING INSURANCE

Underwriters should be aware of potential critical malfunctions of an IT-system resulting from some inherent cause or an accidental or malicious action. These can lead to such things as a catastrophic malfunction of an industrial process or a project design software tool failure. Malfunctions which could

result in simultaneous or delayed physical damage and consequential economic loss will be of interest, since policy cover would attach if not specifically excluded.

For threat analysis, it is essential not only to highlight technical vulnerabilities, but also to consider human elements involved including motivations, attack types, typical scenarios and –stages. These are outlined in section 4.1.

Due to its importance to all types of operational and project Engineering risks, section 4.2 deals with specific “threats arising out of Industrial Control Systems (ICS) vulnerabilities” and section 4.3 deals with “exposure outside ICS”.

This chapter concludes with examples of typical cyber threats to Engineering risks and also loss examples. Latter ones will also be used as a basis to discuss underwriting and claims handling considerations in sections 5. and 6. These sections are a core focus of this paper.

4.1 Threat Factors

Since the dawn of computer networks, hackers have exploited network-provided services for notoriety or personal gain. The exploitation of these systems has only grown, and in an increasingly connected world never more have networks, services, or devices been exposed to these risks.

In a threat landscape where security capabilities have to be continually refined or updated to detect the latest exploitation, the challenge is to maintain the ability to detect malicious events and to innovate defences to provide enduring network protection.

Technical Vulnerabilities

Vulnerability can exist in software, hardware, configuration, or usage of technology and can be activated or used in different ways. The most common access points to vulnerabilities are:

- Tablets, Laptops, Workstations
- Remote Network Users (Wifi)
- USB & Portable Media
- Email Servers
- Border gateways / Firewalls
- Network & Server Infrastructures
- Directory Servers

Vulnerabilities come in all shapes and sizes, just as technology itself does. There are widely different patch (fix) times, but in general, industrial systems environments only patch about 18 months after the initial patch is released. This is largely because of high availability requirements of the machinery and associated operational technology components. Whilst necessary, it is also at odds with having a more secure system in the longer term.

There are mitigating technologies that can reduce risks during these vulnerable transitional periods such as network security monitoring. Encouraging vendors to test for more vulnerabilities before deployment through auditing of their secure coding practices would also help.

Computer Emergency Response Teams

There are organisations dedicated to responding to all types of computer incidents. One that should be of particular interest to the reader of Engineering based insurance is the Industrial Control System CERT in the USA [1]. Another of note, would be the Siemens Product CERT, where Engineering underwriters could learn of vulnerabilities and patches in Siemens products. These are only two examples, but there are over 600 CERTs worldwide who provide a variety of services to their constituents. Some of them provide metrics or data that should be of use to insurance and risk

[1] https://ics-cert.us-cert.gov/ See also Appendix 8 for further explanation

management professionals. A good resource to learn about CERTs worldwide, would be the Forum of Incident Response and Security Teams, at FIRST.org.

EXPLOITS

An exploit is the method or procedure for detecting and taking advantage of a vulnerability which in turn has an effect. The effect and the vulnerability are independent. An exploit turns a vulnerability into an 'unexpected effect' such as the creation of a hidden user on a computer, a remote connection, or a change in the process of the computer controls.

It is difficult to anticipate the very extensive effects that a capable, motivated, malicious engineer/ hacker may visit on a system.

INDUSTRIAL CONTROL SYSTEM (ICS)-, EMBEDDED-, AND CYBER-PHYSICAL SECURITY

In the past most exploits have focused on virtual effects; moving money from a bank account, changing the flow of internet traffic, taking pictures from people's webcams. Over time, the cost of computers and networks fell, and there are ever cheaper smaller computers capable of intermingling with sensors and actuators. Those microcomputers became embedded applications in industrial systems and led to the rise of a new field of computer security: Cyber-Physical security. This important distinction and innovation occurred, because it was now possible to hack things in order to open doors, to cool buildings, or to destroy generators remotely. The effects became physical as computers became embedded in the physical world with physical processes.
The CO2 (Controllability, Observability, Operability) framework helps conceptualize the security or insecurity of cyber-physical systems. This allows people new to the subject to get some idea of the dangers of insecure Operational Technologies (OT).

WHAT CAN GO WRONG IN MANUFACTURING OR INDUSTRIAL ENVIRONMENTS

Controllability	Observability	Operability
Inability to bring the process or system into a desired state. Example failures include: • Control network not in a controllable state • There is no longer a control sequence which can bring the system into an intended state • The sequence of the control commands is unknown to the operator (because it has been altered or potentially altered) • Actuator has lost connectivity or power	**Inability to measure state and maintain situational awareness. Example failures include:** • Inability to monitor sensors (data integrity loss and/or loss of availability) • Untrustworthy measurement (data has lost veracity) • Measurement of all necessary quantities at the right locations is no longer possible • Inability to interpret the measurements e.g. changing the language of alerts	**Inability of the device to achieve acceptable operations. Example failures include:** • Inability to maintain optimal operations under attack • The physical device has been damaged e.g. motor burnt out, gear teeth ground down, pressure vessel burst • Inability to safely shut down • Multiple operators working against each other through same control channel

Table 4.1.1 CO2 (Controllability, Observability, Operability) framework

THE THREAT ACTORS

The threat actors out there are varied in skill set, motivation, and infrastructure. Some hack for fame, some for profit, and some for nationalism or other ideologies. In fact, much of cyber-crime has become an underground economy, and you might not be dealing with the same groups exclusively through what appears to be a single incident. This is because the underground economy has diversified, with different people producing **malvertisements**, and others performing post-exploitation of the machines themselves to harvest valuable data from them.
The good news is that most threat actors don't know how to monetize attacks against engineering environments. That is likely to change over time though. Consequently, the two most severe threats are extortion or nation state sabotage. These threats are not frequent (as of writing only a handful of

incidents are known). However, they are entirely possible. The more frequent events are simple malware infections and cleanup costs, or other more standard cyber-attacks. However, if geopolitical stability were to shift, or more hackers were to bring their focus to engineering environments a great deal of damage might be done before these environments had better defences.
Different types of attackers and their motivations are described in the Appendix 2.

ATTACK TYPES AND SCENARIOS

A small sample of attack types is given below to aid thinking about pricing criteria in respect of different frequency and severity distributions and also for consideration of accumulation risks.

Types of Event	Scenario
Targeted Attack: *Defined target with a specified purpose*	Malicious Act /Targeted Virus
	Distributed Denial of Service (DDoS)
	Extortion without (known) event/threat
Untargeted Attack: *Scalable through automatization (e.g. Spam mail).* *Potential to cause accumulation loss*	Computer Malware, Widespread Virus
Undefined or accidental	Human Error (unintentional operation)
	Disclosure of Data (even via lost laptop, USB stick)
	System Failure (even without human interference)
	Other

Table 4.1.2 Examples of types of cyber-attacks and typical scenarios

ATTACK STAGES – COMPUTER SECURITY MODEL

Underwriters and Claims handlers should also be aware of the timeline of cyber-attacks when discussing loss occurrence.

Threats occur in up to seven stages that can take months or even years to reach their conclusion (Reference: Lockheed Martin Cyber Killchain Document[2]):

1. Reconnaissance *- The attacker finds a gap in security of the social network*
2. Weaponization *- builds a malicious attachment*
3. Delivery *- and delivers it using social media or email targeting an employee*
4. Exploitation *- The employee opens the file and the vulnerability is exposed*
5. Installation *- Malware immediately installs on the client*
6. Command and Control *- The attacker takes control of the system*
7. Actions on Objective *- and is able to pinpoint and access target objective*

Not all threats need to use every stage, and the actions available at each stage can vary, giving an almost unlimited diversity to attack sets.

4.2 CYBER THREATS ARISING OUT OF INDUSTRIAL CONTROL SYSTEM (ICS) VULNERABILITIES

Industrial control systems (ICS) is a term used collectively to describe various types of computer-based systems that control operations of industrial processes, from energy plants and steel mills to bakeries, bottling plants and public transport.

The ICS´s hard- and soft-ware supervises and monitors process parameters by measuring and acquiring process data. It controls an industrial process by managing equipment and machines and giving commands to actuators. An installation is thus operated autonomously in a stable and secure mode.

ICS were originally designed for reliability, safety and functionality to ensure a continuous, fail-safe operation of industrial processes. The fundamental ICS design was performed at a time when communication networking was not usual. Consequently, due to the formerly existing air gaps-

[2] http://www.lockheedmartin.com/us/what-we-do/information-technology/cybersecurity/tradecraft/cyber-kill-chain.html

between ICS and any potentially unsecure world area networks (such as the internet), cyber security was of little concern.

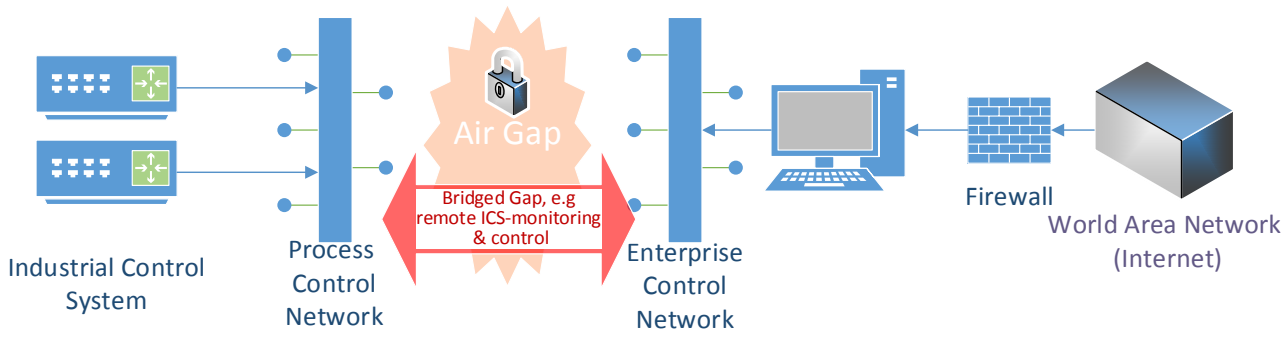


Fig. 4.2.1: Air gap and bridged gap between ICS and WAN (Internet)

Nowadays, the links between ICS and local area- and world area IT networks have become an important cost-saving potential with many features that allow ICS to be used for remote monitoring and control of critical industrial systems. Consequently, there is an opportunity where ICS, that use digital communications networks, can be exploited, turning these features into vulnerabilities.

Those vulnerabilities are being increasingly exploited: "We see more and more hackers that are gaining access to that control system layer," says an official of the Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[3]. ICS-CERT helps US firms investigate suspected cyber-attacks on industrial control systems as well as corporate networks.

But even if the theoretical separation between the process control network and a world area network (WAN) is achieved and protected to a maximum by firewalls, there is always a possibility to bridge this gap, e.g. by attaching USB sticks or Laptops directly to the process control network. This is still a usual method to patch ICS software, e.g. in case of ICS system upgrades.

Further vulnerabilities of ICS become obvious, if one compares different operating conditions of the enterprise and office IT versus the process IT environment including ICS - within one and the same industrial company:

Operating conditions	Enterprise- and Office-IT	Process-IT (ICS)
System lifecycle	3 – 5 years	5 – 20 years
Malware protection	Common	Not common and only with manufacturers permission
Patch management	Common (sometimes daily updates)	Seldom[4]; only with manufacturers permission
System changes	Regularly	Seldom (highly safety regulated)
Availability	Failure and reboot possible	24/7/365-operational

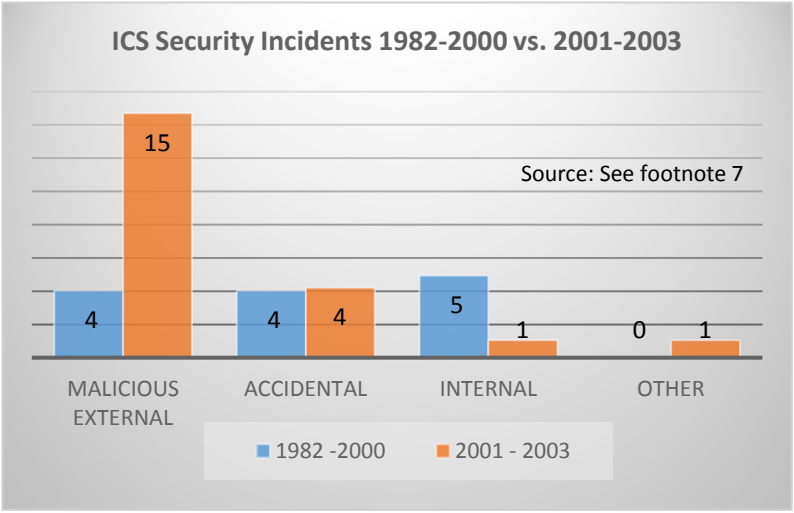
Table 4.2.1: Comparison of Operating conditions in an Enterprise- and Process-IT Landscape.

All the above mentioned vulnerabilities can lead to failures of the ICS. The impact of an ICS failure – be it caused intentionally from outside i.e. by hacking, or even unintentionally from inside i.e. by human error - can be dramatic and material damage can be significant, as will be shown in some loss examples later in this paper and some studies on failures to rotating equipment, i.e. in power plants[5].

The vulnerability and loss exposure of industrial processes and infrastructure via ICS is constantly increasing. According to Dell's annual threat report, worldwide cyber-attacks against ICS/SCADA (Supervisory Control And Data Acquisition) systems doubled from 2013 to 2014[6].

[3] http://www.advisen.com/tools/fpnproc/fpns/articles_new_1/P/252126772.html
[4] http://www.controlglobal.com/assets/Media/MediaManager/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf
[5] http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/?printmode=1
[6] https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf

On a more long-term perspective, this trend is supported by a historical analysis in the paper "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems"[7], published in 2004.



In its analysis of the ratio between accidental to malicious events, there was a clear step change in the number of incidents from malicious causes after 2000. Additionally, external events began to happen more frequently, but losses from malicious insiders were higher, according to the paper.

Fig. 4.2.2 Changes in ICS Security Incidents – long-term perspective

In view of ICS vulnerabilities, more underwriting attention should be directed towards the associated exposure. In reviewing standard questionnaires and standard clauses for Engineering covers it is clear that the IT component is hardly mentioned and has little to no meaning. This is an underestimation of the increasing importance of IT in industrial processes and infrastructure. Potential loss scenarios attributable to increasing interconnectivity of and remote access to industrial control systems are also under-evaluated.
Recommendations on how to assess IT related aspects for ICS is addressed in section 5.1 – Technical Risk Assessment.

4.3 Where is the Exposure outside of ICS in Engineering Policies

Cyber is not just an operational exposure, it can also be a risk during other phases of an engineering project. Some examples of where this risk lies are detailed below, and whilst these are hypothetical examples of what could go wrong, they highlight areas that are of concern to an underwriter.

When people think of Industrial Control Systems they tend to think of the larger control systems such as power plants, but it's important to consider smaller temporary operation technologies such as cranes, forklift automation, cement mixers, traffic systems redirection, which could also be a source of losses.

Cyber risk can be present anywhere technology and software are used within the project. Beyond industrial control systems, some other examples are:

- Logistics Software - for the delivery of equipment to site and stock control,
- Design Software – e.g. Computer Aided Design (CAD), Building Information Modeling (BIM)
- Diagnostics tools used in commissioning, maintenance and decommissioning
- Scheduling and planning – for example PrimaVera software
- HVAC and Building Management systems – for example to circulate oxygen in mines
- Alarms – for example H2S in a petrochemical plant, high wind alarms on cranes
- Payment systems used in payroll or human resources projects associated with engineering

Imagine a policy covers the construction of a new prestigious landmark building. It is a design and build contract and the contractor is using BIM. A disgruntled engineer, who is being paid by a rival

[7] http://www.controlglobal.com/assets/Media/MediaManager/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf

country to disrupt the project, with access to the system, alters the load bearing calculations. He manages to get this signed off by the senior engineer by showing him the legitimate calculations and swapping the manipulated project files after it's been signed. The CAD files go to the contractors and many months later during the early construction, weaker supports than originally designed are used. This causes the building to collapse once the higher floors are added. The loss adjustor and accident investigators do not automatically consider a cyber cause so it is many months until the original files are compared and the deception possibly discovered.

Diagnostic software is often used in the commissioning phase to test and calibrate equipment. For example, a generator can be tested for over-speed and under-speed conditions. Imagine a hacker compromises this software and creates dangerous conditions to alter the speed of the generator causing catastrophic failure during the commissioning phase.

Purchasing of second hand plant and equipment also opens up new risks. Imagine that a piece of equipment is infected in its previous life at a facility. It is possible that the engineers discover the infection or identified it as a root cause, and later sold the equipment second hand. If it is then purchased and gets connected to the new plant, the infection can restart in a fresh operational environment. Even if there is no property damage, there is an associated cost from cleaning up the malware of associated machines.

Every external contractor who goes on site is a potential threat to the cyber security of the project. This risk extends to the maintenance period when a contractor visiting site can inadvertently carry an infection in with them on CD's, USBs, mobile phones or diagnostic software.

4.4 Examples of Vulnerabilities in the Energy Industry

Example 1 : Cyber Vulnerability in Oil & Gas, Petrochemical and Chemical Plants

The Oil & Gas, Petrochemical and Chemical industry is a part of the strategic infrastructure of a nation. Most of the industry´s plants are controlled by computer systems and communicate via on-site, wireless interconnection. As such, Engineering underwriters should consider this industry a potential target for cyber criminals. Depending on the company's investment cycle, patch management and general IT-security awareness, their vulnerability is dynamic and could come from outside as well as from within the organisation.

Moreover, the lifecycle of many chemical plants and refineries is at least 20 – 25 years. Many of them run with old, tailor-made software, with few security updates performed during their lifecycle. Nowadays, process controls are upgraded to standard operating systems with all their vulnerabilities and exploits known to hackers.

Most processes in the Oil & Gas industry are continuous processes which run uninterrupted until a major scheduled maintenance shut-down. This occurs every 4 – 6 years in a refinery.

The spectrum of cyber-threats could stem from intentional hacking by a disgruntled employee, external intentional hacking to an unintentional programming error.

Once a cyber-attack is detected in a Petrochemical / Chemical plant or Refinery, an instant halt of the respective process is not feasible, since it could trigger environmental consequences of spills of chemicals or the flaring of gases. A process shutdown in most cases needs to follow a controlled procedure. In case of a sudden process stoppage, however, e.g. due to hacking, it may take weeks to bring the plant back to normal operation mode.

Consequences and economic loss from a successful cyber-attack could include:

- stolen intellectual property (information of recipes, suppliers, vendors, clients, order volume, pricing and much more)
- material spill and release of gases (pollution of the environment),
- over-pressurized / over speeding equipment with following physical damage and/or environmental pollution

- uncontrolled reactions leading to fire and explosions with massive destruction.

Some of the above may potentially be followed by several months of costly shut-down for cause investigation by the company and / or the authorities and the repair period, including related business Interruption losses. This cyber initiated damage could even exceed regular Vapor Cloud Explosion (VCE) Probable Maximum Loss (PML) scenarios assumed by Oil and Gas underwriters, if multiple simultaneous physical damage were triggered within the same facility by a cyber incident.

A region could also be destabilised if such an "energy" source were to be put out of action following a cyber-catastrophic event.

Professional hackers are already focusing on selling their information / hidden access into companies networks on the dark net or they may be instigating blackmailing campaigns against the company with ransom as their reward.

So far, we haven't seen any reported big losses following a cyber-attack to this industry, but this does not mean that they haven't taken place. The insurance industry should consider the possibility of significant losses – possibly destabilising the financial economy of a nation – triggered by an event which is hard to predict.

This extreme event threat scenario should be part of the whole risk assessment, underwriting and premium calculation process going forward.

EXAMPLE 2: CYBER VULNERABILITY IN HYDRO POWER PLANTS

Hydro Power Plants are a prone target for cyber criminals. There are three different ways to access an automated system:

- Through physical access by an individual into the plant, control room and near the equipment.
- Through the internet. Most plants are connected to the internet to allow remote controlling and logging of maintenance parameters e.g. to the companies headquarter, service vendors or if the plant is in a distant area difficult to access.
- During testing, commissioning, maintenance, shutdown or idle period, service technicians from the vendor, contract technician or in-house maintenance personnel gain access and control to either specific equipment or the overall automation system where they exchange data and information or upload new firmware to the components. During that period they could easily plug in malware-contaminated USB sticks into the control system.

4.5 NOTABLE EXAMPLES OF INCIDENTS, LOSSES AND CLAIMS IN ENGINEERING LINES

While it is important for brokers, risk managers and underwriters to consider possible and probable loss scenarios, it is also important to assimilate lessons learned from real loss examples. Databases on cyber incidents and losses can be found in the Internet. One source specializing in cyber incidents is the RISI database [8].

Hereafter, selected loss examples are discussed, some of them with consequences of physical damage. Each case starts with an abstract and from there lessons learned and points to consider are derived.

4.5.1 LOSSES FROM OPERATIONAL RISKS

2014 STEEL MILL – HACKERS CAUSE PHYSICAL DAMAGE

In December 2014 the German government's Federal Office for Information Security (BSI) released their report on annual findings. In one case they noted that a malicious actor (a common term used in

[8] http://www.risidata.com/Database/event_date/desc

computer security) had infiltrated a German steel facility and was able to cause physical damage and consequential business interruption.

He used a spear phishing email with document attachment embedding malicious code to target the on-site industrial operators. By this method the actor remotely gained access to the corporate network and subsequently into the process network. The adversary showed knowledge in ICS and was able to cause multiple components of the system to fail. Critical process components became unregulated and the furnace was then unable to be shut down properly while in such abnormal conditions, which resulted in significant physical damage.

This incident again highlights the vulnerabilities of the ICS system to malicious cyber-attacks. To determine if the furnace failure itself was an intended result of the cyber-attack, a complete and thorough forensic investigation would have been necessary.

This loss was claimed as physical damage loss to insurers without mentioning the cyber root cause. It shows how difficult it might be:

- to identify cyber losses in silent All Risk Engineering covers
- to apply effectively exclusions if a cyber cause is not notified, and
- even if CL 380 exclusion endorsement is part of the policy conditions, to exclude physical damage, if it was caused inadvertently (see also 5.3.2 CL 380 discussion)

2015 Power Grid Blackout – Hackers Cause Power Outage

On December 23rd 2015 the electricity supply stopped in 103 cities in Ukraine. 186 further small villages had partial black-outs. Overall, more than 200.000 people were without electricity for hours, leading to widespread non-physical damage business interruption. Several IT-Security experts in various countries as well as the German Federal Authority for IT Security are convinced that the incident was caused by a Cyber-attack[9].

This proved to be a very complex three-tier attack:

1) Spear fishing with malware attachments,
2) uploading of additional malware to install remote control via a command-and-control-centre
3) application of software named „Killdisk“ which manipulates process steering and sends false information that systems are working. At the same time, important information was deleted, so that computers could not be restarted.

In addition, an attack on telephone hotlines with Telephony Denial of Service (TDoS) ensured that notifications by consumers were not possible.
Who perpetrated the attack? One week before the attack Ukrainian nationalists had cut the electricity supply lines from Ukraine to Crimea. It remains guesswork and conjecture as to who might be responsible.

Some thoughts for a risk/insurance discussion: Is it war? Is it terrorism? Would an attack be excluded from normal Cyber policies? A majority of experts thinks that it would, but the insurer would have to prove that it was a terrorist or war incident. How can you prove it? It is very difficult and would require extensive forensic efforts.

[9] IT-Security Company iSight reports that since 2013 hacker group „Sandworm" has attacked various targets in the Ukraine and in other European countries. Amongst others, Ukrainian authorities have been targeted, but also European telecommunications companies and even NATO. IT researchers report that the hackers have used their malware also for attacking industrial plants. The specific malware used to attack the Ukrainian power supplier is called "Black Energy 3". It is malware specifically designed for Cyber espionage, not for common Cyber-crimes.

2008 Tram Derailment – Teenager Crashes Trams With a Remote Control

A 14 year old hacked the tram track switching system in Lodz, Poland. He spent a few weeks understanding the infrared track switching system that was usually managed from on board each tram by the driver. He used a universal remote control which he modified slightly. He then used it to record and replay the infrared commands that caused the trams to switch tracks.

This mischief caused several derailments, and at least one collision between passing trams, injuring passengers and causing physical damage. This incident serves as a wake-up call to the danger of remote substations or equipment in the field. Such equipment needs to be secured and the consequences of abusing it understood.

Risk implications: The same infrared technology as used in the tram has many applications in construction, energy and engineering. For example, a safety monitoring system can be used at a site consisting of mobile sensing devices for detecting workers' approach, transmitter sets and repeaters for sending the detected information to a receiver, and exclusive software for interpreting this information. A malicious actor could take control of the system using ordinary and readily available control devices and cause it to misinterpret, delay or stop detecting or relaying sensitive information to the software system hence disabling safety features.

Emerging three-dimensional (3D) sensing video range cameras on construction sites are being used to model, detect, and track the position of static and moving on-site objects in real time. Should this system be subject to a cyber-attack, the attacker could disable or worse still, manipulate the system to provide faulty data and analysis. This could have catastrophic results causing physical damage and/or serious injury to personnel.

2005 Daimler-Chrysler – Virus Causes Inadvertent Physical Damage to 13 Plants

In August 2005, 13 US manufacturing plants were shut down by a simple Internet worm. Despite professionally installed firewalls separating the Internet, the corporate network and the process control network, the Zotob worm had made its way into the control system (probably via a connected laptop). It generated process network traffic that adversely affected the automotive plant´s robotics. Once in the process control system, it was able to travel from plant to plant in seconds.

50,000 workers were unable to work at the production line as it became unsafe, which resulted in $14M in cost of lost production. Physical damage was limited to equipment breakdown and consequential business interruption. However, there was also a financial impact on third party just-in-time suppliers.

While the worm was never coded to affect an industrial control system, the plant operators didn't patch the ICS because they assumed that these were "air-gapped". See 4.2 - ICS vulnerabilities.

Risk considerations: This type of incident could lead to a significant defect in the finished product (through small variations of design specifications, e.g. regarding stability due to missing welding points) which may not be noticed or detected during final inspection stages. Instead, the defect may lead to serious physical damage and/or related failures of the product that may not be directly attributed to a cyber-attack.

Furthermore, many types of production equipment contain safe-lock components that are designed to prevent equipment failure under certain conditions. Components susceptible to these types of attack include thermostatic devices, pressure-, level- and temperature-sensors, counter-balance devices and others. Should such sensor data be altered through an attack on a robotic manufacturing process, then a failure could cause serious physical damage. A similar mindset of loss scenario could also be applied when thinking about Internet of Things (IoT) environments and places where smart tooling already exists e.g. in the aeronautical industry.

2001-2002 Water Treatment System – Former Employee Releases Sewage

Vitek Boden, a disgruntled Watertech company worker, began a campaign of sabotage on the radio communications between wastewater substations. These attacks occurred on at least 46 occasions and resulted in over 3 million litres of wastewater being released into parks and streams. In one case it flooded the lobby of a hotel, causing physical damage and significantly impacting local tourism through the “loss of attraction” of this hotel.

He was eventually caught, but only because of the persistent efforts of one very diligent and persistent engineer. Initially other engineers thought the system was “glitchy”.

Risk thoughts: This incident highlights a number of similar threats to other types of industrial properties. For example, if the incident occurred at a foundry and the attacker communicated with substations controlling the flow of product, they would be able to stop the flow which could easily lead to solidification of products in channels which would then result in significant physical damage.

Similarly, an attacker could abruptly shut down the processing plant in a water treatment facility, causing significant amounts of sludge to accumulate in conveyors moving the product to and from incinerators. Should this attack occur during a cold season, there would be significant risk of physical damage to the conveyor channels.

In these cases, it is important to appreciate that physical damage may have been initiated by a cyber-attack to the plant´s ICS.

4.5.2 Losses from Project Risks

The following loss example is the only one the working group found in the project category. Underwriters should consider that such risks are present dangers, and while they have not materialised or been discovered in larger numbers yet, it does not mean that they will not happen.

2011 Concentrated Solar Power plant – Negligence causes Physical Damage

During final commissioning, the construction project suffered physical damage in excess of USD15M and several months delay in start-up loss amounting to more than USD20M, after one of two booster heaters for the steam feed to the turbines suffered a fire.

Forensic investigation indicated a failure in some ICS - Programmable Logic Control (PLC) modules, which prompted the contractor to bypass some critical safety features. As a consequence the temperatures in the booster heater increased beyond safety limits without being detected.

No malicious intent was suspected at the plant. Instead, the error was blamed on lack of coordination between the supplier and the contractor.

Those considering project risks should be aware that the manipulation of ICS can result in significant physical damage and delayed start-up losses, which would be covered in standard CAR EAR policies, even if cyber is excluded. Standalone cyber policies however, cover losses originating from “human error” and “system failure” being non-malicious causes outlined above.

During testing and commissioning, it is not uncommon for contractors and suppliers to disable certain safety features to either simulate special operating conditions or allow commissioning of parts individually rather than a system. It is also not unusual for strict security controls to be either delayed or intentionally disabled to allow access to systems being commissioned. Under these circumstances, inadvertent or malicious manipulation of ICS and their safety features can result in physical damage consequences.

5 Underwriting Considerations

An understanding of Engineering lines and a solid foundation in underwriting them provides an excellent grounding for tackling the challenging issue of cyber exposures.

Specific to cyber, there are additional considerations not to be ignored when cyber exposure needs to be understood, evaluated and respective cover subsequently written by Engineering underwriters.

These considerations include knowledge of: cyber market, cyber product (i.e. Gap Covers), coverage design (incl. wordings and exclusions), IT vulnerability and security risk assessment, pricing and claims issues (notification and cooperation, forensic investigation). A detailed list of skills and knowledge recommended for Engineering underwriters is provided in Appendix 7.

Cyber Cover needs to be analyzed before underwriting them via different types of cover. The most usual ones are:

- Stand-alone Cyber Cover (Cyber-only policies)
- Affirmative Cyber Endorsements (i.e. write back covers)
- Silent Cyber Exposure – Gaps in Explicit Cyber Exclusions
- Silent Cyber Exposure – Policies without cyber exclusions

In the underwriting process, understanding the cyber risk and its exposure is usually the first step.

Technical Risk assessment including analysis of cyber vulnerability, threat event, accumulation scenario and IT maturity and security aspects are decisive factors which usually influence cyber pricing. Once the risk assessment is performed, the risk can be benchmarked with the insurer´s cyber risk appetite. This will be dependent on 'vulnerability' and 'attractiveness' of the industry for hackers.

Wording considerations will cap and clearly ring fence the exposure of the original risk, depending on coverage elements, limits, deductibles and other parameters (occurrence definitions). As such, wording assessment is essential and its importance cannot be overstated: the policy wording conditions will determine whether an economic loss to the insured will be paid out by the insurer. Underwriting results and premium adequacy is driven by the loss ratio. Additionally, wording conditions can usually modify the pricing depending on scope of coverage, exclusions, conditions precedent, obligations, etc.

Depending on both aforementioned points, adequate pricing will determine if a cyber book of business will support the insurer´s cyber risk return in the long run. Even if good risk selection is performed and wording conditions limit the exposure, whatever the resulting loss ratio, it remains a fact that adequate premiums need to be collected.

Even with an intention of fully excluding cyber risks, Engineering underwriters should realize that below a certain 'nuisance' threshold they may find themselves paying for cyber losses, as the cost of a root cause analysis will outweigh the benefit of paying for that analysis and applying the analysis may result in a legal dispute.

Unintended consequences are often a friend of laxity and sloppiness. They should be avoided. Full awareness of the foregoing and consciousness regarding the following risk considerations will inform an assessment whether deciding to underwrite or to exclude cyber risks.

5.1 Technical Risk Assessment, Risk Appetite

A technical risk assessment supports an underwriting decision whether or not to write a risk and also influences the capacity to be made available, the pricing and certain insurance conditions.

Ideally, the following criteria should be considered when assessing cyber risk from a technical perspective in Engineering insurance:

- **Exposure:** Much depends on the type of engineering risk object (e.g. operational power plant or construction site project) and the potential attractiveness for malicious actors to inflict harm, damage or simply create havoc. Malicious actors' motivation can arise from the challenge of the complexity of a risk or even from knowledge of existing vulnerabilities and corresponding exploits (see also section 4.1 - Threat factors). Legal aspects and the political situation of different countries and/or involved companies can heighten attractiveness for attackers.
- **Complexity:** is to a large extent dependent on the cyber scenarios to be assessed, starting from the root cause (e.g. initiated with a phishing E-mail) and developing to physical damage effects at plant´s equipment or machinery. Complexity is also influenced by the technical

environment involved in this path from cause to effect. This technical environment includes the number of sites and data centres, number of employees, network topology, hardware and software, operating systems, firmware etc. including their vulnerabilities, number of SCADA/ICS sensors/devices, number of IT systems, number of internet connections as well as the grade of connectivity.
In a nutshell, complexity is the dimension which slows down malicious hacks and limits them or magnifies them. It can limit or aid the attacker.
Methods such as Fault Tree Analysis (FTA) and Failure Modes and Effects Criticality Analysis (FMECA) may support an in-depth and systematic scenario- and dependency analysis, if the necessary information detail is available to underwriters. Measuring and grading such complexity, however, is extremely challenging. It might therefore be appropriate to simplify and cluster complexity grading into 'low', 'medium' and 'high'.

- **IT security and maturity:** This aspect of assessment can be based on international IT security frameworks (e.g. ISO 27001, NIST, COBIT, ISF, VDS, GSHB, UK´s Centre for the Protection of National Infrastructure (CPNI) Good Practice Guide for Process Control and Supervisory control and data acquisition (SCADA) Security). For instance, according to the North American National Institute of Standards and Technology (NIST), the following categories are considered in the IT security and maturity assessment:
  - *Identify*: means that a process of identifying and dealing with exposure and complexity of a risk is in place and a risk management methodology is defined and implemented to quantify risks (loss amounts, occurrence probabilities, vulnerability, risk matrices).
  - *Protect*: means that adequate IT security measures are in place to compensate as far as possible the identified risks (Examples for measures: access restrictions, employees security awareness, security policies, firewalls and configurations).
  - *Detect:* means ability to recognize timely any abnormal conditions, hacking, system failures etc..
  - *Respond*: Once a malicious act has occurred and is detected, e.g. an intrusion via a Trojan horse, further effects of such an attack (taking control of an ICS and causing physical damage) can be prevented.
  - *Recover:* System cleanup can be performed, Business continuity management is in place, systems are patched and normal operation is recovered.

Taking into account above dimensions Exposure, Complexity and IT Security/Maturity, a very simple systematic and quantified risk assessment might look as follows:

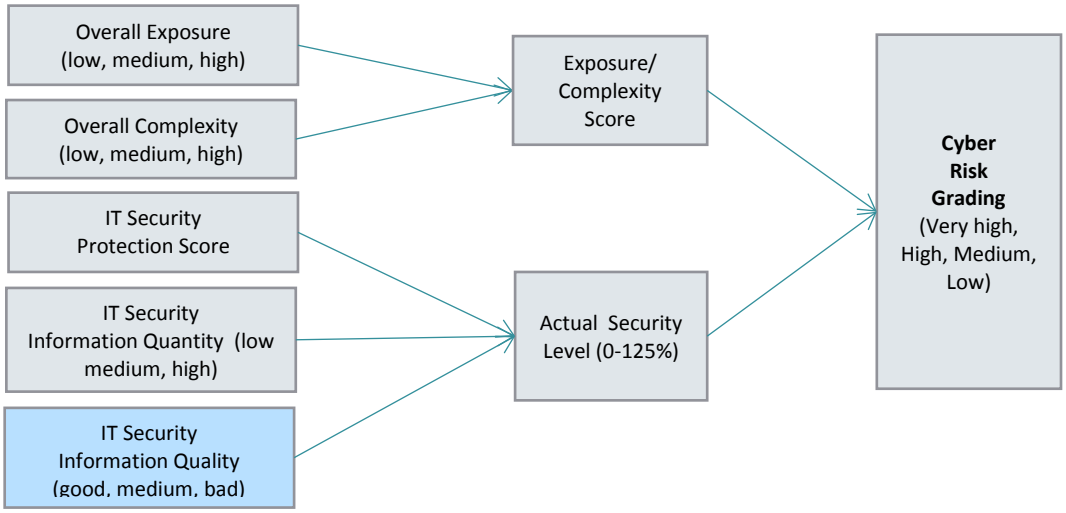


Fig. 5.1.1 Technical Risk assessment based on Exposure, Complexity, Security and Maturity

The quality of cyber risk grading is dependent on the information grade available and the validity of its intermediary results i.e. Exposure/Complexity grading and Security level. It should go without saying

that the higher the financial cyber exposure and capacity written, the higher the validity of cyber risk grading and the higher the IT security level should be.

Underwriters in their practical day-to-day life, however, often have to rely on less than reasonable information (e.g. from questionnaires) to perform a risk assessment, e.g. due to the insured´s reputational or confidentiality constraints. This is particularly the case for sensitive information like risk complexity and IT-security, where one would need deep insider-knowhow from an insured´s IT-security-expert perspective e.g. regarding system hard & software, configurations, firewall settings etc.

Therefore it is recommended as a minimum, to focus on the implementation of good IT security practices and standards (e.g. ISO 27001 certification and others specialized to ICS networks), since they help to evaluate, control and mitigate the cyber exposure of Engineering risks.

For this purpose, the above cited IT security standards are the most common frameworks and provide guidance for cyber risk-assessment (e.g. ISO 27005). They require IT security responsibilities within the insured organization, they define hard- and software requirements as well as procedures for defense-in-depth strategies, system monitoring, forensic plans, incident response, disaster recovery, training and code of conduct of employees and suppliers. A reference of IT security standards and most common ICS/SCADA related best practices is also provided in Appendix 3 – ICS/SCADA Technology, Standards and Good Practices.

Apart from security standards and codes of practice, the most important measures include the level of risk awareness of the insured's employees and suppliers as well as having an established risk culture in place, because currently most attacks start with phishing emails.

Project Risks underwriters should additionally be aware that IT security might not be fully deployed at an early stage of risk. For instance, material damage due to cyber can occur during the project phase, when design- or project management software is corrupted (e.g. BIM, CAD) or when control systems of contractor´s plant and machinery (cranes, tunnel boring machines) are manipulated or adjusted - intentionally or unintentionally.

Also in the commissioning phase, where on-site and remote operators and engineers have access to the ICS to adjust values and set-points and constantly start up and shut down machines via the ICS. IT security that is not fully implemented obviously increases the criticality and vulnerability of such a risk.

Even after commissioning, when an Engineering risk is in its operational phase, the ICS often remains connected to the corporate network for monitoring or to the internet for remote maintenance.

The risk assessment criteria described above, are also helpful in defining the Risk Appetite. A risk appetite could be high if risk exposure is low & complexity is high and its IT security rates very good. On the other hand, with a high exposure, low complexity and low IT security, an underwriter may even want to abstain from writing a such a risk.

5.2 Accumulation Risk Management

Engineering project- and operational risks are usually quite dissimilar regarding their cyber exposure within an insurers Engineering book of business. Cyber-attacks targeting physical damage at a single risk require a prior study of risk-individual industrial processes or critical project phases and so will in most cases have a-single-risk-limited exposure[10] for one insurer.

However, if large scale attacks like cyber terror and cyber war were considered as simultaneous malicious acts, those could lead to cyber catastrophic scenarios, which would either be:

[10] There might be effects of PML exceedance due to cyber for a single risk. I.e. at a refinery, a simultaneous cyber-attack at different critical refinery controls could trigger a higher loss than was assumed by an underwriter for a single vapor cloud explosion Probable Maximum Loss (PML) scenario.

a) limited to geographic regions, i.e. if physical damage targeting attacks were carried out on several neighbourhood electrical substations and power-plants leading to regional blackouts, or

b) geographically spread if hackers got to know how to hack ICS from specific vendors, and perform physical-damage-targeted attacks globally on multiple installations which use one and the same type of critical hard- and software.

Engineering underwriters should be aware of such potential loss accumulation within their insurance company´s book of business. They should be conscious of multiple physical damage and business interruption losses triggered by external communication- and power network failures, e.g. outage of internet.

To repel or mitigate accumulation, it is common practice to exclude worst case cyber cat scenarios with uncontrolled accumulation potential (e.g. external network (Internet) failure or widespread virus and cyber war) via appropriate exclusions in the insurance conditions.

5.3 Policy Wording Considerations

The policy wording should clearly define all the terms regarding the indemnification of a loss. A good understanding and application of such wording construction is also a success factor for cyber underwriting.

The most important sections include the operative clause, the exclusions, the endorsements (e.g. as vehicle for a write back), the loss occurrence provisions, claims notification and cooperation (including evidence of time sensitive losses and –access to documentation and network).

The following sections concentrate on exclusions and write back provisions, as they are most decisive IF a loss is covered. Special attention is drawn to Cyber War and Cyber Terror. Those types of cyber losses may not be frequent from an historical perspective, but underwriters may assume that such would be effective and costly due to involvement of professionals carrying out such attacks.

Apart from exclusions, other policy conditions may determine HOW and to WHAT EXTENT a loss may be covered.

5.3.1 Cyber War and Cyber Terror

The Internet allows interaction with people, websites, programs and machines which can be very distant. A key feature of a cyber-attack is that hackers can be remote in time or space, often in other countries or even on other continents.

The attribution problem of cyber is widely documented and discussed in the computer security whitepapers. It is expensive and time consuming to prove the motive and intentions of agents you cannot identify.

Engineering All Risk covers normally exclude war and terror, whilst they cover losses caused by sabotage and malicious acts. Although the intention of a cyber-attack can be very diverse - it can have a “war-like” character, a terrorist background or a sabotage intention - the way cyber-attacks are planned and performed can appear to be similar or even identical. Digital and network forensic work is complex and can be expensive and is hardly ever done when indemnifiable physical damage occurs. It is therefore questionable if it makes sense to distinguish between acts of war, terror or sabotage for losses caused by a cyber event when the origin and motivation of an attacker can be disputed.

5.3.2 IT and Cyber Risks Exclusions

In the absence of any specific exclusion, all risk policies will cover physical damage resulting from a cyber incident. If underwriters wish to exclude such risks then they need to do so in clear terms.

There are several exclusions and clauses in common use in the Engineering insurance market, dealing with cyber and Internet liability. It is worth noting that it is typically for insurers to prove that

the exclusion applies, therefore in order to take advantage of the exclusion the insurer must be prepared to spend the costs for digital and network forensics to prove that IT and cyber are the root cause of a physical damage. Although many of these wordings have been written into policies for some years, it should be noted that they remain legally untested, so it is unclear how effective they would be in practice.

For technical risks, the most frequent cyber and IT exclusion clauses are discussed below (see full wordings in Appendix 4):

- **NMA 2912**

  NMA 2912 excludes loss due to damage or impairment to computer systems, except if caused by Fire Lightning Explosion Aircraft or vehicle impact falling objects (FLEXA) and Natural Hazard (NatHaz) perils as set out in detail in the wording. If an explosion, for example, results in damage to a computer system, then consequential losses are covered.

  In common understanding, computer systems, hard-software etc. would also include Industrial Control Systems (ICS). However, these terms are not defined in the clause, so there could be some scope for debate. It is also uncertain whether the clause would be broad enough to exclude liability where physical damage resulted not from the damage or alteration of an industrial control system, but merely from its normal operation – for example where a hacker operated an industrial control system to open a valve on an oil pipeline, causing a leak.

- **NMA 2914 AND 2915**

  1. Exclude cost, expense for repairing/replacing, and also physical damage resulting from lost/damaged data or software.
  2. Cover physical damage caused by fire/explosion, where the fire/explosion results from lost/damaged data or software.

  The difference between the two clauses is in the valuation. In case of physical loss or damage to IT hardware (electronic media) caused by an insured peril, the following is stipulated: NMA 2914 covers the IT hardware plus restoration and re-engineering of data and software. NMA 2915 only pays for the IT hardware plus the copying back of backed up data and software, but no restoration or engineering costs are covered.

  It is important to note that the exclusion is focused on the loss of electronic data. Data is defined in the clause, and is said to include software. This means that a cyber-attack, which is focused on causing physical damage by manipulation of an industrial control system, rather than alteration or destruction of data, will not necessarily be excluded by the provision.

  Additions are sometime made to this list of perils, which would extend the scope of physical damage cover beyond fire and explosion. Particularly, attempts of additions like “Malicious damage” or even “All Risk Perils” have been observed in some markets. Those would invalidate the exclusion of physical damage due to a “malicious” or all risks” cyber cause and also undermine any underwriting approach to exclude and write-back cyber (gap) covers.

- **CL 380**

  CL380 is the widest of the exclusions, and is in common usage in upstream energy policies. It excludes all loss, damage and liability directly or indirectly caused by, contributed to by, or arising from, the use or operation "*as a means for inflicting harm*" Information and Communication Technology (ICT) as set out in detail in the clause (see Appendix 4). The terms are not defined in the exclusion.

  The one, narrow, exception to this is, where the policy covers war and/or terrorism, in which case the exclusion will not apply where a computer or software has been used in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

Although industrial control systems are not expressly mentioned, the clause is so broadly worded that they would probably come within the definition. It should be noted that the exclusion will only apply if the cyber-attack has been carried out "*as a means for inflicting harm*". If, for example, a hacker where to inadvertently cause physical damage whilst they were logged onto the insured's computer system for another purpose, then arguably such physical damage would not be excluded. This could be the case in the 2014 Steel-mill case, see section 4.5.1.

It will be to insurers to prove that the attack has been carried out "*as a means of inflicting harm*", and this is likely to prove extremely difficult in practice.

5.3.3 Advanced Cyber Exclusion Clause

It is clear from the above that the cyber exclusions currently used by Engineering underwriters will not necessarily be sufficient to exclude all instances of physical damage caused by cyber- incidents or any other damages or losses resulting from cyber incidents. With this in mind the working group has prepared an alternative exclusion for the consideration of Engineering underwriters who do not wish to underwrite cyber risks. See Appendix 5.

The exclusion 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.

The capitalised terms are defined in the exclusion.

Computer Malicious Act is defined as "any wrongful act carried out through the use of Data, Computer Systems or Computer Networks" and expressly includes denial of service attacks. Unlike CL380, there is no need for insurers to demonstrate an intention to cause harm on the part of the hacker, only that the hacker's acts are "wrongful". This would therefore exclude an attack such as that on the German steel mill, where it is believed that the physical damage was an inadvertent result of the hacker's activities on the insured's computer network.

The second key element of the exclusion is that it makes payment of any claim, not just a 'cyber claim', subject to a condition precedent regarding preservation of data and access to the insured's computer systems. This is designed to 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 or not.

5.3.4 Write-back Endorsement

Should an underwriter want to exclude damage (including physical damage) from an All Risks Engineering cover via the Advanced Exclusion Clause (Appendix 5) in a purpose to provide an affirmative cyber write-back cover, an example of a simple write-back wording is offered in Appendix 6.

In case of other exclusion clauses used, when writing-back cyber cover it is recommended to bear in mind the following aspects:

What is the risk object?

There are two ways of defining the trigger of a possible cyber-cover. By defined cyber-peril scenarios like virus, malicious act, DDOS etc. or by creating an all risks solution. Both solutions have advantages and disadvantages:

	Positive	Negative
Named scenarios	Insurer is protected from unwanted changes in risks	The insured bears the risk of changing risk-landscape
All risks	Broad cover, that can adapt to the constant changing risk-landscape	Risks are changing and may be unintentionally covered

WHEN IS THE COVER TRIGGERED?

There are different moments, when a possible cyber-cover can be triggered. The challenge with cyber-risks is, that not all moments are visible to the insured.

	Pros	Cons
Infection	Broadest timeframe that can be covered	Difficult to notice and prove, when exactly the infection took place
Detection	If malware etc. is detected it can be removed before causing any damage	Tough to prove whether the insured did detect the incident at the time they should have detected it.
Damage Occurred	Infections, that have not caused a damage yet, are not covered	Moral hazard, because the insured has no benefit to remove an existing but not yet harmful infection
Claims Made	Motivates the insured to detect and report an incident as soon as possible	The insured can suffer from gaps in the cover through a late trigger (e.g. a wind-turbine is slowed down by a cyber-attack and the insured detects this after nearly a year)

For Engineering risks with physical damage focus, only “Damage Occurred” within the effective policy period is relevant.

5.4 KEY CRITERIA IN PRICING

Traditional Engineering lines pricing is usually retrospectively derived from loss and exposure data. Often this involves a detailed, object-specific analysis (e.g. gas-turbines). Such analysis would include the following parameters:

- **loss frequency** (e.g. how often are combined cycle power plants hit by machinery breakdown losses in average per year of their operation)
- **from-ground-up loss severity and distribution** (what is the minimum, maximum and average loss amount, which proportion of the exposed values has been damaged by a loss?)
- **exposure data** (such as sums insured and probable maximum loss)

If you want to create effective cyber pricing in the traditional way described, you would need to collate cyber loss data with the above attributes.

Contemporary loss data for cyber events are incomplete, as many of such cyber events are often not published in order to protect confidentiality and reputations.

One recommended general concept for Cyber Pricing is a Monte Carlo simulation[11] of original, “from ground up” cyber loss events, using a collective pricing model with an industry-specific, scenario-based approach.

Industry-specific cyber loss scenarios have to be identified and defined. One such scenario would be a “Malicious Act through IT systems to cause property damage”. Other malicious scenarios might include a “Distributed Denial of Service (DDoS), causing a non-physical damage business Interruption” to an industrial plant. Such an event would not be covered by a traditional Engineering policy due to the absence of a physical damage trigger.

[11] https://en.wikipedia.org/wiki/Monte_Carlo_method

For Engineering risks, at least the following cyber scenarios need to be considered:

a) covered by most Engineering policies if not specifically excluded:
   - Malicious Act /Targeted Virus; Target: Physical Damage and consequential Business Interruption (BI)

Fig 5.3.1 Scenario and triggered Indemnification Forms (IF)

   - Human Error with Physical Damage Effects
   - System Failure with Physical Damage Effects

b) excluded in most traditional Engineering policies, but may need to be covered in future cyber add-on covers if not specifically excluded:
   - Malicious Act /Targeted Virus; Target: Non-physical damage BI (excl. PD)
   - Denial of Service (No virus and no change in data): Business Interruption (excl. PD)
   - Disclosure of Data (revealing nuclear power plant technical information)
   - Extortion without (known) event/threat

The main structure of the 'from ground-up' pricing can be implemented as a table with scenarios (in columns) and affected cover sections (in rows) as in the example below:

Table 5.3.2. Sample Cyber Scenarios (columns) and affected cover sections (rows)

Scenarios are e.g. a "Malicious act/Targeted virus: Target PD" or "Human Error". If they occur and are technically successful, they trigger different sections of the coverage. Each of those sections covers several Indemnification Forms (denoted IF; for example, an event could lead to Physical Damage which triggers PD costs but also system restoration costs) and Consequential BI (Loss of Profit and Increased cost of working).

For every scenario, an @Risk (TM) simulation tool mathematically simulates the number of events and which coverage sections and indemnification forms are affected. The breakdown from scenario to IF follows a "dependency tree" (see Fig. 5.3.1) in order to account for dependencies (hence no estimation of correlations is required). The actual costs are then simulated at the end (leafs) of the

scenario tree (these are the IFs) using applicable loss severity distributions, which are predefined by experts.

With this method, rating frameworks for typical Engineering cyber covers and policy structures can be created in order to simplify the underwriting of risks for which the effort of an extensive risk assessment and expert simulation cannot be justified.

For such standard risks, the idea is to use the expert based approach and determine “Expected Loss” net rates per standard cyber coverage for a set of typical policy structures in the market.

The advantage of above described pricing models is their flexibility. Scenarios can be easily adapted to the dynamically evolving threat factors and the indemnification forms, as the markets and cyber policy formats change. On the other hand, one needs to balance the recurring effort to estimate parameters by experts in order to keep pricings up to date in this dynamic environment.

It goes without saying that the quality of results of net pricing rate should be improved through a periodic calibration of rates with actual loss data.

From commentary in the following section, the costs of investigating incidents in order to allow underwriters to rely on any exclusion also needs to be factored into the gross rating structure.

6 CLAIMS CONSIDERATIONS

Operational and project engineering claims are often, by their nature, complex. Moreover, Engineering claims where cyber exposure is involved introduce a further layer of complexity.

It will not always be clear to insurers whether the physical damage and business interruption claim has been caused by a cyber incident. Therefore, if insurers want to successfully rely on cyber exclusions or limits, and if there are indications that a cyber-attack may have been the root cause of the claim, then a timely cyber forensic investigation of the loss is crucial.

In the majority of jurisdictions the onus of proof is on the insured to prove that the requirements for indemnification under an insurance policy are fulfilled, but the onus of proof rests with the insurer to establish that an exclusion applies. If cyber risks are excluded under the policy, it will therefore be upon insurers to demonstrate that the loss was caused by cyber-attack and is not covered.

Special case: Silent Policies without exclusions. Because an Engineering policy is generally on an “All Risks” basis, in the absence of a cyber exclusion any loss or damage to property insured caused by a cyber-attack would be covered. No specific cyber root cause investigation would be necessary and the respective claims management and adjusting process will be the same as for any other physical damage loss under that policy.

6.1 SUCCESS FACTORS IN CYBER CLAIMS MANAGEMENT

For all operational and project Engineering covers with the cyber underwriting approaches “Like it”, “Leave” it or “Change it”, as laid out in section 3, successful cyber claims management generally depends on the following:

- Develop a mindset that includes thinking of cyber as a possible cause for any claimed physical loss or damage. If you suspect that this is the case, consider appointing a cyber forensic specialist.
- Any claim with regard to a physical loss or damage caused by a cyber incident depends on the occurrence of such a loss or damage within the policy period, irrespective of the fact that a malicious code or malware may have been introduced or a hacker may have accessed the IT systems of the insured prior to the commencement date of the policy.

  Be aware that some jurisdictions classify the corruption, manipulation or deletion of data as physical damage, such that the introduction of a malicious code or malware or the access by a hacker to the insured’s IT systems may be determined as a physical loss or damage by a

court. In this case, the introduction of a malicious code or malware or the access of a hacker to the insured's IT systems must have occurred during the policy period in order to claim such a physical loss or damage.

Note: In order to avoid such a claim the insurer should clearly define within the policy that data shall not be considered as insured property.

- Timeframes are important if insurers are to secure evidence – logs, screenshots, witness statements, particularly in view of the relatively long incubation or preparation period of a malicious act in Engineering risks. For this purpose, insurers need to ensure that they have access to such evidence via the claims notification and cooperation clauses, and subsequently appoint appropriate IT analytics. Access to evidence should include other necessary IT components. These could include corporate networks, servers, as well as cloud service providers (which are not part of the insured policy, but may be considered necessary for investigation). During their investigations, forensic experts may face challenges in getting access to sensitive systems and IT-security details, in view of the insured´s reputational risk which may depend on good IT-security.
- Clear instructions are necessary for claims management, whether and when to involve a loss adjuster or a claims service provider. Having a network of service providers and forensic experts is important for insurers and loss adjusters alike.
- The clearer insurance policy conditions are, the more straightforward claims can be managed and adjusted. This applies particularly to exclusion and write-back approaches, where clarity regarding insured perils, insured interests and insured objects is paramount. It cannot be stressed strongly enough that clarity is achieved through unambiguous definitions for terms such as cyber incident, data, property damage, loss and occurrence. Additionally, see the definitions provided in the Advanced Cyber Exclusion Endorsement in Appendix 6. In a rapidly evolving environment, such definitions should be regularly reviewed to ensure that they are still fit for purpose. Clear policy conditions also include rights and duties in case of loss.

6.2 PARTICULAR, CASE DEPENDENT CLAIMS MANAGEMENT REQUIREMENTS

Considering the above, there are different requirements needed in order to deal with cyber claims related to Engineering lines depending on the "Like it", "Leave it" or "Change it" approach according to section 3:

A) "LIKE IT" AND "CHANGE IT"

The "Like it" (write it consciously) and "Change it" (limit it) approaches can be treated together because they differ only in the limitation applicable to the "Change it" approach.

The "Like it" and "Change it" approaches need the active participation of the insurer in case of a claim because a key interest of the insurer might be to mitigate any cyber related losses or damages and ensure that any continuing threat is deleted quickly. This is only possible if the insurer is able to involve - as soon as possible - cyber experts, namely IT service providers. Insurers might offer insureds within the insurance policy a "cyber hotline" to an IT service provider which the insured can use in case of a cyber incident. This way, the insurer can improve the prospect that a cyber expert is immediately involved, if a cyber incident occurs and any loss or damage might be mitigated. Furthermore, the insurer is more likely to get relevant information to deal with a possible cyber related claim. Having a "cyber hotline" in place could be costly, cumbersome and time consuming. The insurer would have to enter into an agreement with an IT service provider, negotiate the required services for the claims management processes, include the cyber hotline and set up all peripheral arrangements (e.g. remote access to the insured's computer systems, the capacity for site visits for technical and forensic investigations, if required etc.). To make use of the hotline of course, the insured would also need to be aware that the physical damage was caused by a cyber-attack.

An IT service provider could be useful if crisis management services for loss mitigation are required. These might also incorporate IT forensic analysis to investigate the causation of the cyber incident and/or the property damaged and enable the Insurer to determine coverage.

Under the "Change it" option, where cyber exclusions cannot be imposed, further limiting policy conditions can be considered. These include the insured´s obligations to comply with IT security standards, conditions precedent, warranties, obligations etc. An unambiguous wording and a detailed IT analysis, as described above, is vital in the event of a cyber claim. Remember: clarity of intent and clarity of wording.

B) "LEAVE IT"

The "Leave it" (exclude it) approach is more of a reactive approach and would, in case of a cyber related claim, dictate an IT forensic approach to secure evidence to illustrate that the damage is the result of a cyber-attack. Once this is proven then further detailed analysis of the nature, timing, and scope of damage may be unnecessary. This may sound a simple and obvious step in the claims process; however, it is one that is often missed with expensive resources being deployed unnecessarily by both the insurer and the insured to discuss the scope and nature of damages when from the outset the wording of the cyber exclusion clause would be sufficient to decline an indemnity.

Also consider that there can be situations where in light of a rather small claim, the investigation costs compared to the loss would not justify further costs to decline a claim under the operation of a cyber exclusion.

C) CONCLUSION

Whichever approach is adopted, the involvement of a cyber forensic expert or other experts is essential when faced with a loss caused or thought to be caused by a cyber-attack. Insurers are commended today, to establish sound contractual relationships with such experts. In this way, they will be better prepared for future cyber claims management and react quickly to preserve crucial evidence.

Another key message is that insurers need to find a way to consider from the outset whether cyber may have played a role in an incident presented and if so, they should have a mechanism to react accordingly.

An insurer can also consider outsourcing the entire claims management to a cyber skilled loss adjuster. A downside of this approach is that it could lead to additional costs and loss of time which is key when it comes to a cyber incident at the site of the insured.

7 EMERGING RISKS FROM INTERNET OF THINGS (IOT) AND CLOUD SERVICES

Traditional Engineering lines are focused on physical effects and most cyber risk currently appears not to cause physical damage. However, this is changing, very quickly. Actions taken on a computer halfway around the world can be directly relevant to the way turbines spin, motors are optimized, and robotic assembly lines are configured. With the Internet of Things (IoT), the physical world is becoming one big information system, where data is mostly processed and stored "offshore", e.g. in the Cloud.

At its core, the IoT is a simple concept: objects or even construction materials are connected to machines or devices through electronic tags and hooked up to the Internet, thus enabling several objects to communicate with each other. In this hyper-connected system, data can be captured on, for example, the availability of steel, iron and cement and used to pre-empt supply chain downtime or to monitor the health of machinery, allowing for early maintenance and repairs[12].
In 'smart' or energy-efficient buildings sensors and data analytics manage energy consumption and reduce operating costs. Significant amounts of sensors are used to detect machine faults and through IoT, preventive maintenance is scheduled automatically.

[12] http://www.strategic-risk-global.com/how-construction-businesses-are-benefiting-from-the-internet-of-things/1416535.article

However, such innovation has the potential to be highly disruptive. A hyper-connected construction site, with hundreds of connected objects and devices – is open to cyber risk. Systems can be attacked by outsiders if no protection is in place. Critical operating and security systems can be shut down: examples are fire and camera security systems or even sprinkler systems, which can be controlled and switched off through the Internet.

The reasons for this high disruption potential? Possibly design criteria that were too optimistic, seeking to minimize human intervention in processes or closed loop controls for the sake of cost reduction and reliability. A downside is that criteria with very short time-to-market requirements often disregard scenarios where malicious actors could take action to cause out-of-specification operation modes never considered in the "fail-safe" design of such autonomous systems.

A conservative underwriting approach would consider physical damage in such scenarios. However, this fails to inform the underwriter about how cyber impacts Engineering lines until after damage occurs. ICS-CERT reported 215 incidents in 2015. Most of these incidents did not have any physical damage, as such, they are ignored. However, today's malware that does not cause physical damage, could very well be precursors of more direct impacts on the safe operations of control systems in the future.

The decision process is more complex than a simple cost-benefit comparison. Current non-damage activities may become so advanced that physical damage will result at some point in the future. Understanding the impacts of 'non-damage cyber' today might very well enable better risk management/risk transfer before physical damage becomes more common in the IoT and Cloud environment.

8 BALANCE OF INTERESTS BETWEEN INSURANCE NEED AND -SOLUTION

Cyber-awareness of both underwriters and insureds are factors in facilitating a balance of interests between cyber insurance needs and solutions. This awareness will allow effective cyber insurance covers to be written and accepted.

Due to the rapidly evolving nature of cyber threats, the emerging risks from connected IoT systems and associated losses in Engineering lines, it is important that the insured´s risk management encompasses a cyber threat analysis; this could create the basis for cyber risk assessment and tailor-made cyber covers.

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).

In this context, all players, who, for whatever reason, insist on the inclusion of cyber or removal of cyber exclusions from covers, without going through an appropriate risk assessment and premium analysis will only serve to drive those covers into non-profitability in the long run.

How can the dilemma be solved?

Effective communication and dialogue! A risk dialogue amongst all partners (insureds, insurers, brokers, etc.) can greatly help to discuss risk needs and to seek bespoke risk solutions and covers. It is important that the partners have an adequate knowledge of cyber so that they can talk from a common understanding.

Insurers and brokers who advise insureds on how to mitigate risk by consulting, and offer tailored solutions for the remaining risk, is a promising approach.

Keeping risk management at a strategic level is key. As in Machinery Breakdown insurance, where cover should not be a substitute for preventive maintenance, a cyber insurance solution should not replace solid IT security standards.

Finally, a beneficial common goal for all, would be the creation, application of and adherence to good IT security standards which make life hard for malicious actors and could reduce the frequency and

severity of cyber-attacks. Recommendations thereto are provided by US and European authorities in respect of critical infrastructure and resilience See various links (see Appendix 9, bottom). Within various of those recommendations, a strong role in risk management is assigned to insurance.

Transparency in respect of cyber losses and the sharing of Indicators of Compromise (IoC) to other insureds, after any loss payouts and forensic investigations should be a goal of claims groups. For those unfamiliar with the term IoC, this is about metadata concerning the cyber-attack. It might be names and hashes of malicious files, network addresses used by the attackers, attachments to phishing emails, or malicious URLs. This information can then be correlated and compared with other incidents to help protect other insureds. There are companies who provide and maintain databases of IoCs, and help other companies to use them wisely. For further information on IoC's see[13].

Collection of IoC´s would also maximize the value of the forensic investigations, as malicious binaries and attacker controlled infrastructures could become ineffective much more quickly than they do today. It is by driving up the costs required to mount an attack that all parties, insured, insurer and reinsurer, would benefit.

Malicious infrastructures could only be used a limited number of times. Just as multiple insureds do not want to be victims of a similar attack each, insurers do not want to payout multiple times for similar events if they can be 'nipped in the bud'. One way to do this would be to make sure that Indicators of Compromise are distributed regularly, to assist defenders in blocking, detecting, and avoiding known malicious or mischievous actions.

9 CONCLUSION

With increasing global interconnectivity and the many attendant benefits, there is also a downside. Systems that were traditionally thought safe, and isolated, are becoming connected and hackable.

Threats associated with Information and Communication Technology (ICT) and the Internet are not just an 'insurance issue'. However, Cyber insurance could be the financial component of a global risk management strategy to manage the cyber threats. As ICT and Internet of Things (IoT) becomes more a part of our daily life, so too, Cyber insurance is likely to gain in importance and possibly become a standard part of any corporate risk transfer strategy like health, fire or liability insurances. In future, Cyber may even be a dedicated insurance line individually!

Ignoring Cyber Risk, if exercised, is an option that will be very significant for technical insurers. Risk carriers have to decide how to manage the growing cyber risk from the various threat sources identified (e.g. silent covers in their books of business). Failing to do this will not allow for the creation of an adequate long-term Cyber Risk business model with an appropriate risk return. In particular, it will become ever more challenging to price the risk, and legal uncertainties may make this strategy more complicated in the future.

In view of the exponential technological development we are experiencing, understanding cyber risk and keeping in pace with clear trends is of course, only a first step. Further client- and business oriented actions are necessary, such as initiating cyber dialogue with insureds and risk partners in a "Like it" approach. This client- and risk centred dialogue will enable the partners to develop strategies, appetites and individual risk solutions aimed at achieving a balance between insurance needs and effective risk management.

Beyond the insurance-related dialogue, further technological cooperation between industry and insurers could make insured targets much less attractive for malicious actors. So, for example, this could be achieved through minimizing cyber vulnerability stemming from interconnectivity in IoT ecosystems with improved design, and also post-incident, sharing Indicators of Compromise. Such cooperation, whilst likely difficult to be set up and performed, would ultimately benefit all those interested in helping to avoid losses.

[13] http://openioc.org/

Regardless of which strategy you employ for insurance and Cyber Risk in Engineering, this paper should have amply demonstrated that it pays to know more about cyber risk.

So whether you like, leave, or change Cyber Risk in your insured lines; keep learning, discussing, and re-evaluating Cyber-Risk as well.

APPENDIX 1 – GLOSSARY

Term	Explanation
APT	The Advanced Package Tool, or APT, is a free software user interface that works with core libraries to handle the installation and removal of software on the Debian Linux distribution and its variants. APT simplifies the process of managing software on Unix-like computer systems by automating the retrieval, configuration and installation of software packages, either from precompiled files or by compiling source code.
BIM	Building information models (BIMs) are files which can be exchanged or networked to support decision-making about a place. Current BIM software is used by individuals, businesses and government agencies who plan, design, construct, operate and maintain diverse physical infrastructures, such as water, wastewater, electricity, gas, refuse and communication utilities, roads, bridges and ports, houses, apartments, schools and shops, offices, factories, warehouses and prisons.
Botnet	A botnet is a number of Internet-connected computers communicating with other similar machines in an effort to complete repetitive tasks and objectives. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation.
CERT	Computer emergency response teams (CERT) are expert groups that handle computer security incidents
Cloud	Cloud computing, also known as 'on-demand computing', is a kind of Internet-based computing, where shared resources, data and information are provided to computers and other devices on-demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services
Cyber Risks	This paper defines 'cyber risk' as risks arising from the storage, use, computation, and/or transmission of electronic data. Such cyber risks may be malicious, for example caused by individual hackers or nation states, or inadvertent, for example caused by a coding or an operating error.
Data	Data is a set of values of qualitative or quantitative variables; restated, pieces of data are individual pieces of information. Data is measured, collected and reported, and analyzed, whereupon it can be visualized using graphs or images. Data as a general concept refers to the fact that some existing information or knowledge is represented or coded in some form suitable for better usage or processing.
DLP	Data loss prevention solution is a system that is designed to detect potential data breach / data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). In data leakage incidents, sensitive data is disclosed to unauthorized personnel either by malicious intent or inadvertent mistake. Such sensitive data can come in the form of private or company information, intellectual property (IP), financial or patient information, credit-card data, and other information depending on the business and the industry.
DOS/DDOS	In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service (DDoS) is where the attack source is more than one–and often thousands of-unique IP addresses.
DRP	A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is "a comprehensive statement of consistent actions to be taken before, during and after a disaster."
Exploit	An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to

	occur on computer software, hardware, or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service attack.
Exposure	Potential for damages. An insurance company's potential to provide coverage under an insurance policy
Firewall	In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted
Hacker	Hacker (computer security). People involved with circumvention of computer security. This primarily concerns unauthorized remote computer break-ins via communication networks such as the Internet (Black hats), but also includes those who debug or fix security problems (White hats), and the morally ambiguous Grey hats
Hacktivist	Hacktivism or hactivism (a portmanteau of hack and activism) is the subversive use of computers and computer networks to promote a political agenda. With roots in hacker culture and hacker ethics, its ends are often related to the free speech, human rights, or freedom of information movements.
ICS	Industrial control system (ICS) is a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.
Industry 4.0	Industry 4.0, or the fourth industrial revolution, is a collective term embracing a number of contemporary automation, data exchange and manufacturing technologies. It had been defined as 'a collective term for technologies and concepts of value chain organization' which draws together Cyber-Physical Systems, the Internet of Things and the Internet of Services.
Internet of Things	The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities.
IT – Information Technology	Information technology (IT) is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise.
ITIL	ITIL, formerly an acronym for Information Technology Infrastructure Library, is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL 2011 edition), ITIL is published as a series of five core volumes, each of which covers a different ITSM lifecycle stage.
LAN	A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, or office building. A local area network is contrasted in principle to a wide area network (WAN), which covers a larger geographic distance and may involve leased telecommunication circuits, while the media for LANs are locally managed.
Malvertisement	A Malvertisement is an online advertisement that is infected with a virus or malicious computer code, which takes advantage of placement of online advertising to steadily disperse malware to new users. Malvertisement is a coined word to describe malware advertisement
NAS	A network access server (NAS) is a single point of access to a remote resource.
Patch	A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually called bugfixes or bug fixes, and improving the usability or performance. Although meant to fix problems, poorly designed patches can sometimes introduce new problems (see software regressions). In some special cases updates may knowingly break the functionality, for instance,

	by removing components for which the update provider is no longer licensed or disabling a device.
Payload	In computer security, payload refers to the part of malware which performs a malicious action. In the analysis of malicious software such as worms, viruses and Trojans, it refers to the software's harmful results.
Ransomware	Ransomware is a type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a trojan, whose payload is disguised as a seemingly legitimate file.
SCADA	SCADA (supervisory control and data acquisition) is a system for remote monitoring and control that operates with coded signals over communication channels (using typically one communication channel per remote station). The control system may be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording functions. It is a type of industrial control system (ICS). Industrial control systems are computer-based systems that monitor and control industrial processes that exist in the physical world. SCADA systems historically distinguish themselves from other ICS systems by being large-scale processes that can include multiple sites, and large distances.
Server	A server is a computer program or a machine that waits for requests from other machines or software (clients) and responds to them. A server typically processes data. The purpose of a server is to share data or hardware and software resources among clients.
SQL	SQL Structured Query Language is a special-purpose programming language designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS).
Threat	The possibility of a malicious attempt to damage or disrupt a computer network or system:
Trojan	A Trojan horse, or Trojan, in computing is any malicious computer program which misrepresents itself to appear useful, routine, or interesting in order to persuade a victim to install it. The term is derived from the Ancient Greek story of the wooden horse that was used to help Greek troops invade the city of Troy by stealth.
Virus	A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".
Vulnerability	In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.
WAN	A wide area network (WAN) is a telecommunications network or computer network that extends over a large geographical distance. Wide area networks are often established with leased telecommunication circuits.
Wifi	Wi-Fi (or WiFi) is a local area wireless computer networking technology that allows electronic devices to connect to the network
WLAN	The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network" (WLAN) product based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. However, the term "Wi-Fi" is used in general English as a synonym for "WLAN" since most modern WLANs are based on these standards. "Wi-Fi" is a trademark of the Wi-Fi Alliance.
Worm	A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.

APPENDIX 2 – TYPES OF ATTACKERS AND STAGES OF ATTACKS

TYPES OF ATTACKERS

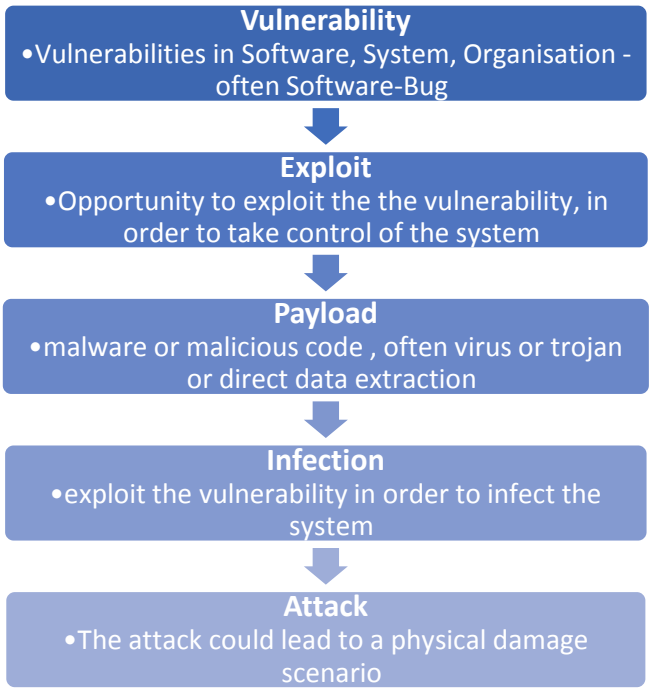
As referenced in section 4.1 - Threat Factors, below table explains different types of attackers, their motivation, objectives and typical attack methods:

Types of Attackers	Objective	Example of Attacks
Hacktivists Motivated politically or socially	Public disclosure	DDoS [1)] SQL-Injection [2)]
Blackmailers Extorting by the threat of exposing a criminal act or discreditable information	Ransom	Ransom-Ware [3)] DDoS
Saboteurs Through subversion, obstruction, disruption or destruction	System failure Public exposure (disclosure)	Trojan horse [4)]
Spies	Extraction of Information	Trojan horse [4)]

Table 4.1.1: Type of Attackers and their objectives.
1) Distributed Denial of Service (DDos),
2) Structured Query Language (SQL) – injection with malicious code,
3) Encryption of essential data causing inaccessibility by users
4) Malicious computer code .e.g. acting as a backdoor to enable unauthorized access to the affected computer

STAGES OF ATTACKS

In most cases attackers will study vulnerabilities in order to achieve their objective. A cyber-attack frequently develops in different stages:



APPENDIX 3 – ICS/SCADA TECHNOLOGY, STANDARDS AND GOOD PRACTICES

ICS - INTRODUCTION

An Introduction by Munich Re to Industrial Control Systems (ICS) and useful guidance for underwriters thereto is provided in the following attachment: ***see Attachment 1 (PDF)***

IT-SECURITY - STANDARDS AND GOOD PRACTICE- REFERENCES:

ISO/IEC 27000 series	Standards for information security management
ISO/IEC 27032	Guidelines for cyber security
ISO/IEC 27033	Guidelines for IT network security

ICS/SCADA- RELATED STANDARDS AND GOOD PRACTICE - REFERENCES:

(Please be aware that links might get outdated, up-dated, changed or taken from the Internet!)

ISA 99/IEC 62443	Standards for industrial automation and control system security
ICS-CERT	Recommendations of the US Homeland Security https://ics-cert.us-cert.gov/Recommended-Practices
NIST SP 800	Cybersecurity Framework -12, -14, -26: Guides to IT security principles, management and controls -82: Guide to Industrial Control Systems Security – *available for free, easy to read and highly recommended* http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
NISTIR 7628	Guidelines for smart grid cyber security and electric power infrastructure – is planned to integrate into ISO/IEC 27000 series.
NERC CIP	– North American Reliability Corporation Critical Infrastructure Protection http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
ENISA (2011):	Protecting Industrial Control Systems - Recommendations for Europe and Member States: ***See Attachment 2 (PDF)***
OSCE (2013):	Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, ISBN 978-92-9235-022- : ***see Attachment 3 (PDF)***
National Security Agency (2015):	Department of Homeland Security, Federal Bureau of Investigation, Seven Steps to Effectively Defend Industrial Control Systemshttps://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf
MELANI	Reporting and Analysis Centre for Information Assurance: Measures for the protection of industrial control systems (ICSs) https://www.melani.admin.ch/dam/melani/en/dokumente/2013/10/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf.download.pdf/measures_for_the protectionofindustrialcontrolsystemsicss.pdf
ENISA	Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors https://www.enisa.europa.eu/publications/maturity-levels/at_download/fullReport https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/maturity-levels
Industrial Ethernet Book (IEB)	http://www.iebmedia.com/ethernet.php?id=8460&parentid=74&themeid=255&hft=68&showdetail=true&bb=1&PHPSESSID=vk9tck0p6rq69jt6d3l6co7lh7
SCADA and Smart Grid Integration	https://www.csiac.org/journal-article/the-efficacy-and-challenges-of-scada-and-smart-grid-integration/
CPNI - Security for Industrial Control Systems	http://www.cpni.gov.uk/advice/cyber/Security-for-Industrial-Control-Systems/
CPNI – SCADA guidance	http://www.cpni.gov.uk/scada/

APPENDIX 4 – DIFFERENT CYBER EXCLUSION CLAUSES

NMA 2912 AND 2928 CLAUSES

See Attachment 4	PDF: NMA 2912 Cyber Non aggregation Clause
See Attachment 5	PDF: NMA 2914 Information Technology Hazard (Risk) Exclusion Clause

NMA 2914 AND 2915 ENDORSEMENTS

See Attachment 6	PDF: NMA 2914 Electronic Data Endorsement A
See Attachment 7	PDF: NMA 2915 Electronic Data Endorsement B

CL 380 CLAUSE

See Attachment 8	PDF: CL380 Institute Cyber Attack Exclusion Clause

APPENDIX 5 – ADVANCED CYBER EXCLUSION CLAUSE

Endorsement – Advanced Cyber Exclusion 2016 (IMIA 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 are 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 **Human Error** affecting the **Insured's Computer Systems**, or

   e) a **System Failure** occurring on the **Insured's Computer Systems**, or

   f) a **Defect** of the **Insured's Computer Systems**, or

   g) 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's obligation to indemnify the Insured in accordance with this Policy is subject to the Insured's fully compliance with all of the following 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

3.2.1 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;

3.2.2 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;

3.2.3 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;

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

3.2.5 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 and the singular shall include the plural and vice versa:

Computer Malicious Act
Means any wrongful act carried out through the use of **Data**, **Computer Systems** or **Computer Networks** with the intention to cause any 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 or network facilities connected via a form of communications technology, including the internet, intranet and virtual private networks (VPN), allowing the networked computing devices to exchange **Data**.

Computer Systems
Means the Information Technology (IT), industrial process control or communications systems, as well as any other item or element of hardware including and IT infrastructure, software or equipment that is designed to be used for the purpose of creating, accessing, processing, protecting, monitoring, storing, retrieving, displaying or transmitting **Data**. The term **Computer Systems** shall also include IT devices such as laptops, external drives, CD-ROMs, DVD-ROMs, magnetic tapes, magnetic disks or USB sticks that are used in **Data** processing to record and store **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 anything of value, including money, or other property or services that the Insured is forced to pay or to provide to the extortionist or any other party.

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, nations, or political entities or organisations by using - wholly or partially - **Computer Systems** or the internet, to render non-functional, 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, redirection, alteration or deletion of **Data** which, when stored or 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 information, irrespective of the way it is used or rendered such as text, figures, voice, images or any machine readable data, including software or programs, that are being transmitted or are 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** or **Computer Networks** being altered or rendered temporarily or permanently non-functional or otherwise unavailable to anticipated users of such **Computer Systems** or **Computer Networks** through the deluging and overloading of **Computer Systems** with an incoming stream of requests or **Data**. The term **Denial of Service Attack** includes a distributed denial of service attack in which a multitude of compromised systems are used to coordinate a simultaneous attack as well as both volumetric and application specific attacks.

Defects
Means any fault, defect, malfunction, error or omission in design, plan, specification, material or programming on or of the **Insured's Computer Systems**.

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.

Human Error
Means any negligent or inadvertent IT operating error, including an error in the choice of software to be used, a set-up error or any inappropriate one-off operation carried out by an **Employee** of the Insured..

Insured's Computer Systems
Means (i) any **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 IT services including **Data** or **Computer System** management, **Data** storage and **Data** processing, software maintenance and/or development for the benefit of or at the request of the Insured on a **Computer System** that is controlled and managed by the IT service provider.

System Failure
Means an unintentional or unplanned - wholly or partially - outage of a **Computer System** not directly caused by a physical damage.

APPENDIX 6 - CYBER WRITE-BACK ENDORSEMENT

The following alternative example can be used along with the Advanced Cyber Exclusion Clause 2016 (Appendix 5):

Write-back Endorsement – 2016 – Alternative 1 (Draft)

Endorsement forms part of Policy No.:xxxxxx

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.

Write-back Endorsement – 2016 – Alternative 2 (Draft)

Endorsement forms part of Policy No.:xxxxxx

Issued to:

Issued by:

Effective:

Endorsement No.:

It is hereby agreed and understood that the Advanced Cyber Exclusion 2016 shall be amended as follows:

Clause 1. and Clause 2. shall be deleted.

All other terms and conditions remain unchanged.

APPENDIX 7 - SKILLS AND KNOWLEDGE FOR ENGINEERING CYBER UNDERWRITERS

Below table lists recommended skills and knowledge considered for successful cyber underwriting in Engineering lines.

Market knowledge: Understands the drivers of insurance demand for Cyber in Engineering lines(mainly 1st party covers but also 3rd party) and is able to analyze the potential of this Line of Business for the specific market Knows and understands the legal context of his market and can draw correlations to the need for certain insurance products in the market
Product knowledge: Understands the threat factors and essential IT technology terms and structures well enough to be able to go into discussions with clients and evaluate underlying coverages Knows the impact of technological developments on different coverage concepts Knows the impact of legal issues on different coverage concepts Has a good know how about different Cyber coverages and the underlying exposures, is able to talk with clients about how they would respond to threat scenarios seen by a client and can tailor a coverage to the needs of specific markets / client groups, etc. Knows the delimitations of Cyber business to other coverages and potential links to other coverages
Coverage design / Wording: Is able to read and understand policy, exclusion and write-back-endorsement wordings and underlying coverages and can draw conclusions / give recommendations, find weaknesses on such, etc.
Risk assessment and pricing: Knows which information is necessary for a proper single risk assessment, knows IT-security standards and understands the reason behind questions of a risk assessment and knows how to evaluate/ whom to involve for evaluating the exposure and risk quality based on the answers given Can derive a risk-adequate price on a per risk basis for the specific cover
Monitoring and accumulation: Knows and understands which information needs to be monitored and gathered / how to monitor accumulation risks and is able to explain this topic to the client (power-grid-blackout scenarios including business interruption).
Claims: Understands how cyber insurance claims arise and the success factors of dealing with such claims, see section 6. Is able to derive conclusion on necessary know how of external service provider and forensic based on underlying coverage components Knows and understands the claims handling process and its cost drivers and is able to translate this into a suitable insurance solution or also application of exclusions, see section 6.
Other: Knowing about Cyber Analytics Solutions Providers and its services

APPENDIX 8 – AN EXPLANATION OF COMPUTER EMERGENCY RESPONSE TEAMS

IT and Internet changed our world in many aspects, also in the industry. Automated industrial plants or infrastructures became standard. In the old days, field devices e.g. valves, motors or sensors were hard-wired individually and connected to the control room. Nowadays, the “eyes, nervous system and brain" of an automated installation is the industrial control system (ICS) where field devices are connected to a network and to computers where the process logic software is running. The ICS (SCADA, DCS, PLC, PCN, PAC, note: acronyms need to be explained, comment from Alex) supervises and monitors process parameters by measuring and acquiring process data and controls a process by managing equipment and machines and giving commands to actuators thus running an installation in a stable and secure mode. The ICS comprises hardware and software and connects all components. A frequently used network topology for industrial applications is a hybrid of bus, star, ring and mash topology.

In emergency cases alarms can activate safety interlocks and the ICS activates the fail-safe logic which brings an installation in a so called "fail-safe state". ICS have often an interface to corporate intranet of a company and most corporate intranets are connected to the Internet. Often it is required to allow remote access to an ICS for maintenance or monitoring reasons. This is how ICS can be hacked from outside and the process logic or interlocks can be manipulated. The impact of an ICS failure – be it intentionally from outside or unintentionally from inside - can be dramatic and material damage can be significant as will be shown in some loss examples later in this article.

The first of its kind, it was dedicated to sharing alerts of vulnerabilities and threat intelligence about hacking groups around the world. In fact CERTs can be corporate, private, or public bodies.

They can function at the organisational level, at the national or trans-national level, or even be sector specific such as REN-CERT. They can be very useful allies to insurers, in particular their yearly reports contain[14] a variety of data that will help insurers understand the risks.

[14] https://ics-cert.us-cert.gov/

APPENDIX 9 - REFERENCES AND WEB-LINKS

(Please be aware that links might get outdated, up-dated, changed or taken from the Internet!)

Description	Link
RISI Online Incident Database	http://www.risidata.com/Database
RISI Twitter News	https://twitter.com/risidb
Hacker hits on U.S. power and nuclear targets spiked in 2012	http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/index.html
The Internet´s most dangerous sites - A hydroelectric plant	http://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/4.html
Energy industry under cyber-attack	http://www.kallanishenergy.com/2015/11/23/energy-industry-cyber-attack/
List of Targeted Cyber Attacks	https://apt.securelist.com
Automated Vulnerability Scanning Tool	http://www.sandia.gov/ccd/projects.html
ICS accessible over the Internet	https://icsmap.shodan.io/
Oil and Natural Gas - CyberSecurity	http://ongisac.org/
New reconnaissance threat Trojan.Laziok targets the energy sector	http://arstechnica.com/security/2015/03/energy-companies-around-the-world-infected-by-newly-discovered-malware/
Fireeye Cyber Threat Map (see Utilities and Manufacturing)	https://www.fireeye.com/cyber-map/threat-map.html https://www.fireeye.com/solutions/utilities.html
Cyber Insurance for Critical Infrastructure:	http://www.tripwire.com/state-of-security/featured/cyber-insurance-for-critical-infrastructure-does-flo-even-know/
US power grid vulnerability from physical and cyberattacks	http://www.washingtontimes.com/news/2014/apr/16/inside-the-ring-us-power-grid-defenseless-from-att/
Cyber security vulnerabilities for the oil and gas industry Lysne Committee study	https://www.dnvgl.com/oilgas/download/lysne-committee-study.html
World´s biggest data breaches: Selected losses > 30.000 records	http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Emerging Claims	http://www.lockelord.net/enewsletter/default4.aspx?archive=yes&showtopics=yes
Iranian hackers 'targeted' New York dam	http://www.bbc.com/news/technology-35151492
Global nuclear facilities 'at risk' of cyber	http://www.bbc.com/news/technology-34423419
How IoT transforms the Insurance Industry	http://www.businessinsider.com/how-the-internet-of-things-is-transforming-the-insurance-industry-2015-7?IR=T
Vulnerabilities from Niagara run networks	https://www.washingtonpost.com/investigations/tridiums-niagara-framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story.html
Cyber Security at Nuclear:	https://www.chathamhouse.org//node/18747
Hackers Find Open Back Door to Power Grid With Renewables	http://www.bloomberg.com/news/articles/2014-07-01/renewable-energy-s-expansion-exposing-grids-to-hacking
THN – The Hacker News	Dragonfly Hackers Target 1000 Western Energy Firms http://thehackernews.com/2014/07/dragonfly-russian-hackers-scada-havex.html
Securing the move to IP-based SCADA/PLC networks	http://www.cpni.gov.uk/documents/publications/2011/2011035-securing-move-to-ip-based-networks.pdf?epslanguage=en-gb
Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience	https://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical
Executive Order -- Improving Critical Infrastructure Cybersecurity	https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
Homeland Security subcommittee calls for strengthened cyber insurance role	http://www.businessinsurance.com/article/20160329/NEWS06/160329792/homeland-security-subcommittee-calls-for-strengthened-cyber?tags=|76|73|302|299
Cybersecurity, Infrastructure Protection	https://homeland.house.gov/subcommittee/cybersecurity_infrastructure_protection_and_security_technologies_subcommittee/
Insurance for Cyber-Related Critical Infrastructure Loss	https://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf
Network and Information Security Directive: first EU-wide legislation on cybersecurity	https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation
EU Agency for Network and Information Security	https://www.enisa.europa.eu/