



LEG London Engineering Group



Cyber Risks – PD/BI Coverage in Industrial Property Cyber Exposure for Power, Energy and Project Risks

London, 16th November 2016

Willis Towers Watson



Agenda

	Item
9.30	Welcome & Opening Remarks Alex Clayton, Construction CEO - Willis Matia Cazzaniga, IMIA EC & Global Line of Business Leader - Zurich Suzan Pardesi, OPERA EC & Onshore Engineering Underwriter - Navigators Jon Wiegand, LEG Chairman & Head Engineering & Construction London - SwissRe Corso
9.45	IMIA WGP 98 (16) Cyber Risks - Engineering Insurers Perspective Alexander Schmidl, Senior Underwriter Global Clients Property - Munich Re
10.30	Cyber – Silent Exposure in Industrial Property Simon Dejung, Senior Underwriter Specialty Line Engineering – SCOR
11.15	Coffee Break
11.30	Panel Discussion – IMIA Draft Advanced Cyber Exclusion Clause Paul Lowrie, Partner - Clyde & Co LLP Aiko Schilling, Senior In-House Counsel Wordings - Munich Re Andrew Herring, Practice Leader Energy EMEA region - Marsh Israel Silverman, Vice President Associate General Counsel - SCOR Markus Bassler, Head of Energy Onshore & Special Risks - Partner Re
12.30	Q&A and Conclusions

Disclaimer

Presentations and material used during the workshop represent the views and interpretations of the authors and editors of the IMIA Workgroup WGP 98 (16) and of the members of the Panel Discussion session.

These do not necessarily express presenters' companies opinion.

All presenters and Panel Discussion members do contribute and present in their own personal capacity as supporters of this IMIA, LEG and OPERA initiative rather than on behalf of their companies.

Third-party sources are quoted as appropriate. IMIA, LEG and OPERA are not responsible for the content of the external sources including external websites referenced in the presentations.

All workshop support material is intended for information purposes only.

Topics discussed are of a qualitative nature and complying with Anti-Trust laws & regulations.

Why the interest?

Potential Costs of a Data Breach

- **Reputational damage**
- **Fraudulent payments or systems/software/data corruption**
- **Regulatory fines and penalties**
- **Legal liability**
 - Class action litigation
 - Financial institutions: card replacement
- **Costs of notification**
 - Forensic investigation
 - Printing, postage or other communications to customers
 - Credit monitoring services
- **Crisis management costs to restore reputation**
 - Legal, public relations or other service fees
 - Advertising or related communications



Why the interest?

Potential Loss Exposures

Transmission of malicious code

- Cost to remediate security vulnerability
- Cost to investigate event
- Liability to customers and other third parties

Sabotage, defacement and vandalism

- Cost to remediate website and other content
- Hourly income while offline
- Liability to third parties for inappropriate content

Denial of service attacks

- Lost income due to a network interruption
- Extra expense to restore the network
- Cost to remediate website and other content

Online extortion

- Cost to remediate security vulnerability
- Cost to investigate event
- Extortion demand

Dimensions of Cyber Risk

HA = Hacking Attack

WA = Wrongful act by employee

	Module	Cause	Cover	Covered Costs
3rd Party	➤ Security and Privacy Liability	HA WA	Legal liability due to violation of data protection obligations	<ul style="list-style-type: none"> Litigation costs (incl. Regulatory proceedings) Defense costs Indemnity payments
	➤ Internet Media Liability	WA	Legal liability due to infringement of copyright or misleading advertising	
1st Party	➤ Privacy Breach Costs	HA WA	Crisis Management	<ul style="list-style-type: none"> Notification Legal advice Forensics PR consultant Credit Monitoring
	➤ Business Interruption	HA WA	Interruption of services	<ul style="list-style-type: none"> Net profit loss System restoration
	➤ Cyber Extortion	HA WA	Introduction of malicious code, D.-o.-S. attacks and disclosure of confidential information	<ul style="list-style-type: none"> Extortion money payments Reward Payments
	➤ Digital data Reconstitution Costs	HA WA	Corruption or destruction of digital data	<ul style="list-style-type: none"> Forensics Reconstitution costs

Cyber Risk in Power, Energy and Project Risks

Potential consequences of Cyber Risk attacks

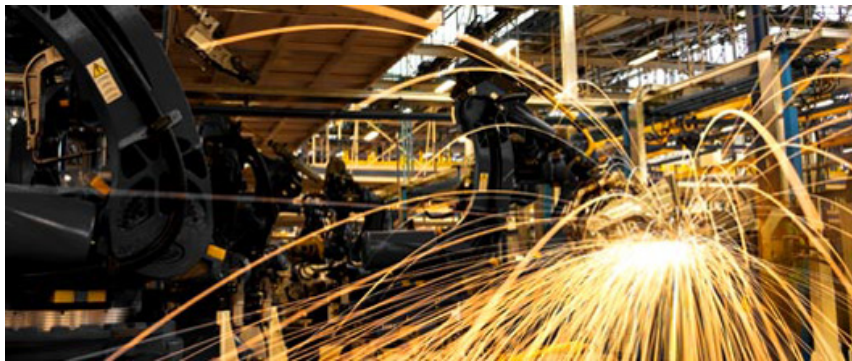
- Intellectual Property (IP) Theft
- Data and Software Loss
- Cyber Extortion
- Cyber Crime/Fraud
- Breach of Privacy Event
- Network Failure Liabilities
- Physical Asset Damage – Property Damage
- Death and Bodily Injury
- Incident Investigation and Response Costs
- Business Interruption (BI) – As a consequence of Cyber Attack or indirect PD
- Market share loss
- Impact on Reputation



Cyber Risk in Power, Energy and Project Risks

Possible Loss Scenario and Industry exposure to Cyber Risk attacks

Manufacturing



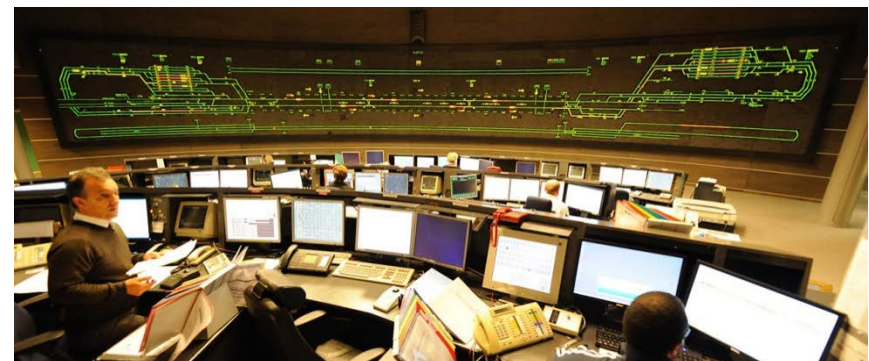
Energy & Utilities



Construction




Infrastructures





Cyber Risks - Engineering Insurers Perspective IMIA Working Group Paper 98 (16)

Cyber Risks – PD/BI Coverage in Industrial Property
London – November 16, 2016

Alexander Schmidl – **Munich RE** 



OVERVIEW



What is it all about?

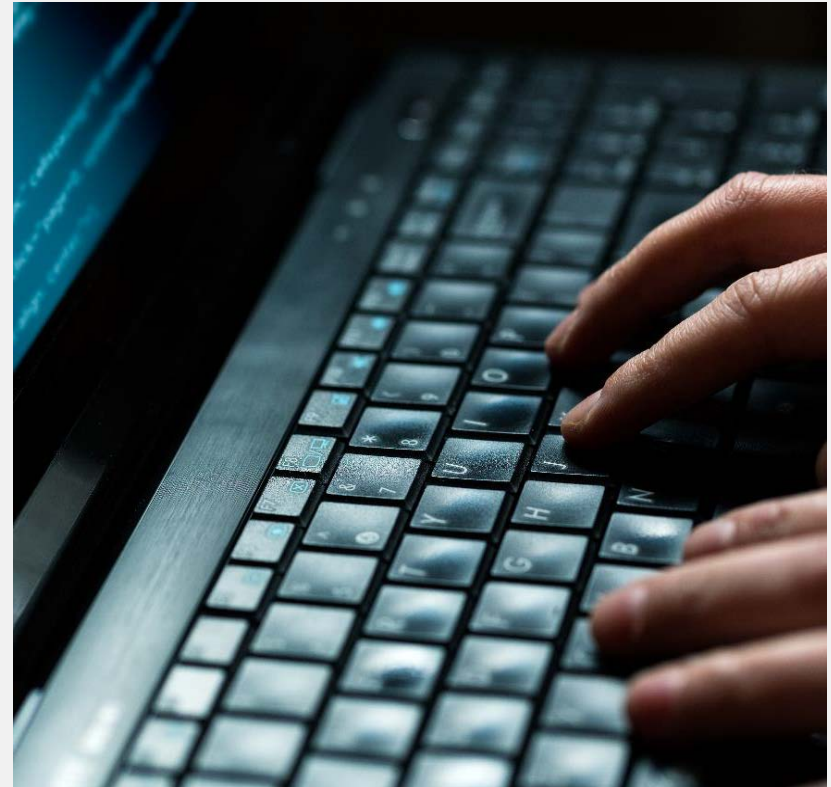
Objectives

IMIA Workgroup

Scope & Content

Some Highlights

Q&A



WHAT IS IT ALL* ABOUT?

*CYBER RISK IN ENGINEERING LINES



Physical damage caused by cyber

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

Physical damage **losses** are paid by insurers

Lack of Cyber underwriting and premium calculation

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

OBJECTIVES OF THE CYBER WORKGROUP



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

Cyber Risks

Engineering Insurers Perspective



Working Group members

Alexander Schmidl (Chair)	Senior Underwriter	Munich Re Munich
Andreas Schindler	Insurance Consultant	GDV Berlin
Anna Woolley	Senior Underwriter Construction	Zurich GC/UK
Ali Arifoy	Associate Director	VHV Allgemeine Versicherung
Eireann Leverett	Senior Risk Researcher/Founder	Cambridge University/Conoinnity 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 – Zurich
Tom Tannion	Managing Director	Overseas NEIL Ltd. Dublin
Mattia Cazzaniga (Sponsor)	Global Line of Business Leader – Engineering Lines	Zurich Insurance Zurich

Rev. A002 16.9.2016

to publish a paper in October 2016:

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

<http://www.imia.com/wp-content/uploads/2016/09/IMIA-Working-Group-Paper-9816-Cyber-Risks-Rev-A002-16-09-20161.pdf>



Working Group Members

Alexander Schmidl (Chair)	Senior Underwriter	Munich Re Munich
Anna Woolley	Senior Underwriter Construction	Zurich GCiUK
Ali Arisoy	Associate Director	VHV Allgemeine Versicherung
Eireann Leverett	Senior Risk Researcher/Founder	Cambridge University/Concinnity Risks
Mamoon Alyah	Managing Director	CEERisk Consulting, London
Pascal Madiba	Vice President	SCOR – New York
Paul Lowrie	Partner	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



1 Executive Summary

2 Introduction

3 A Decision is Needed

4 Cyber Risk in Engineering Line Insurance

4.1 Threat Factors

4.2 Cyber Threats arising out of Industrial Control System (ICS) Vulnerabilities

4.3 Where is the Exposure outside of ICS in Engineering Policies

4.4 Examples of Vulnerabilities in the Energy Industry

4.5 Examples of Incidents, Losses and Claims in Engineering Lines

4.5.1 Losses from Operational Risks

4.5.2 Losses from Project Risks



5 Underwriting Considerations

- 5.1 Technical Risk Assessment, Risk Appetite
- 5.2 Accumulation Risk Management
- 5.3 Policy Wording Considerations
 - 5.3.1 Cyber War and Cyber Terror
 - 5.3.2 IT and Cyber Risks Exclusions
 - 5.3.3 Advanced Cyber Exclusion Clause
 - 5.3.4 Write-back Endorsement
- 5.4 Key Criteria in Pricing

6 Claims Considerations

- 6.1 Success factors in cyber claims management
- 6.2 Particular, case dependent claims management requirements

7 Emerging Risks from Internet of Things and Cloud Services

8 Balance of Interests between Insurance Need and -Solution

9 Conclusion

SOME HIGHLIGHTS

1- Underwriting Decision Options iro Cyber Risk



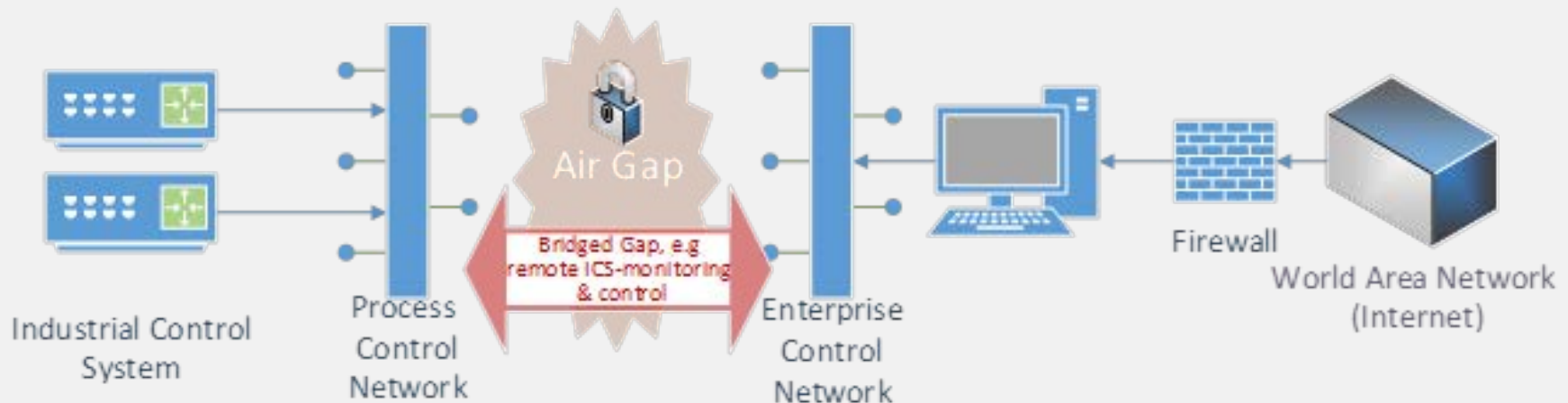
Like it (Price it)	Leave it (Exclude it)	Change it (Limit it)
<p>Provide Cyber cover either via:</p> <ul style="list-style-type: none"> • Standalone Cyber Policy or • Exclusion (see 5.3.3) and Write-back endorsement (see 5.3.4) or • Under unchanged “All risk” engineering policies, assessing and pricing cyber risk. Refer to section 5.-Underwriting Considerations 	<p>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).</p>	<p>Mitigate the risk by</p> <ul style="list-style-type: none"> • 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.
<p>Pro’s:</p> <ul style="list-style-type: none"> • Monetizing market demands • Risk partnering with insured • Adequate risk return 	<p>Pro’s:</p> <ul style="list-style-type: none"> • Minimizing risk in the engineering book of business • Potential for adequate risk return 	<p>Pro’s:</p> <ul style="list-style-type: none"> • Business can be retained
<p>Con’s:</p> <ul style="list-style-type: none"> • Difficult to sell in overcapitalized markets • Adequate cyber pricing is challenging due to lack of historical data, metrics and models 	<p>Con’s:</p> <ul style="list-style-type: none"> • Difficult to enforce • not a useful risk solution for the insured • remaining risk not monetized 	<p>Con’s:</p> <ul style="list-style-type: none"> • Difficult to enforce • Still not charging premium for exposure. • Potentially not meeting clients expectations

SOME HIGHLIGHTS

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



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



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

SOME HIGHLIGHTS

3- Discussion of Engineering Cyber losses 1/2



4.5 EXAMPLES OF INCIDENTS AND LOSSES IN ENGINEERING LINES

4.5.1 LOSSES FROM OPERATIONAL RISKS

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

2015 UKRAINIAN POWER GRID BLACKOUT - (BI - LOSS)

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

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

2001-2002 MAROOCHYSHIRE – (PD – LOSS)

4.5.2 LOSSES FROM PROJECT RISKS

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

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

SOME HIGHLIGHTS

3- Discussion of Engineering Cyber losses 2/2



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

<https://www.youtube.com/watch?v=OVMwl2TWrZw>

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

SOME HIGHLIGHTS

4 – Advanced Cyber Exclusion and Write-Back Endorsements



Endorsement – Advanced Cyber Exclusion 2016 (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/or 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**.

SOME HIGHLIGHTS

4 – Advanced Cyber Exclusion and Write-Back Endorsements



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

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

- a) **Damage to or Loss of Data** occurring on the Insured's Computer Systems,
- b) **Computer Malicious Act** on the Insured's Computer Systems,
- c) **Computer Malware** on the Insured's Computer Systems,
- d) **Human Error** affecting the Insured's Computer Systems, or
- e) **System Failure** occurring on the Insured's Computer Systems, or
- f) **Defect** of the Insured's Computer Systems, or
- g) **Cyber Extortion.**

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

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

SOME HIGHLIGHTS

4 – Advanced Cyber Exclusion and Write-Back Endorsements



Note:

- The burden of proof for applying an exclusion is on the insurer and for that
- successful investigation about cyber as root cause is key

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

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

SOME HIGHLIGHTS

4 – Advanced Cyber Exclusion and Write-Back Endorsements



IMIA WORKGROUP WRITE-BACK ENDORSEMENT 2016 ALTERNATIVE 1 (DRAFT)

Issued to:

Issued by:

Effective:

Endorsement No.:

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

SOME HIGHLIGHTS

5 – Success Factors in Claims Management



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

SOME HIGHLIGHTS

6 – Balance of Interests between Insurance Need and -Solution



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

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

How can the dilemma be solved?

Do you know it?



THANK YOU!



Cyber – Silent Exposure in Industrial Property

A representative discussion for the entire industry?



Simon Dejung

London – November 16, 2016

DISCLAIMER

The opinions expressed in this presentation represents the views and interpretations of the author and do not necessarily represent the official position of SCOR.

Third-party sources are quoted as appropriate.

This publication is intended for information purposes only.

Topics discussed are of a qualitative nature such as the impact of new legislation and complying with Anti-Trust laws & regulations.

we will focus on...

- Consequences of interconnectivity
- Legal environment
- Wordings for industrial property up to date for current exposure?
- Onus of proof - What is the price to exclude cyber?
- Are loss adjusters, claims handlers and risk engineers familiar with cyber?
- Think about: cyber - war, terror, inadvertent IT failure

IoT & Interconnectivity in our everyday's life



There is expected to be **75 billion** connected devices by 2020.

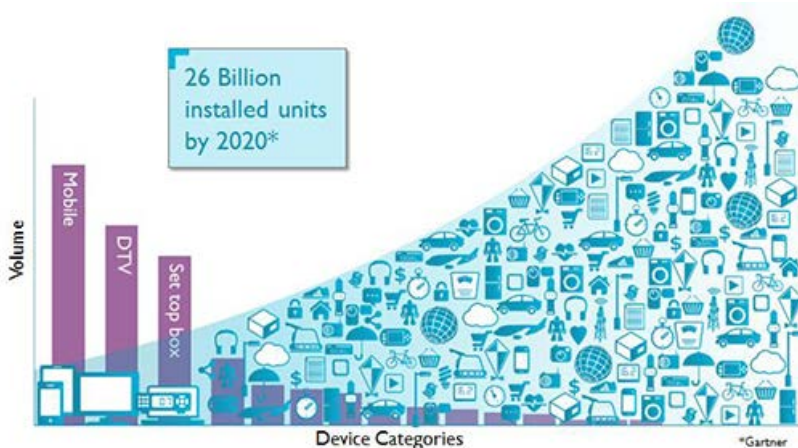
Friday's Massive DDoS Attack Came from Just 100,000 Hacked IoT Devices

Wednesday, October 26, 2016 Swati Khandelwal

G+ 45 Share 1114 Tweet 292 Share 129 share 1600

Analysis Of Friday Attack

Future DDoS Attacks Could Reach 10 Tbps



EU & US - Protection of personal data

EUGDPR.org The Regulation The Process More Resources Our Partners

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.

TIME UNTIL GDPR ENFORCEMENT UTC
562:17:10:21
 Day Hr Min Sec

GDPR Portal: Site Overview

Quick Links

This website is a resource to educate the public about the main elements of the General Data Protection Regulation (GDPR)

GDPR Key Changes
 Summary of key changes

FEDERAL TRADE COMMISSION
 PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connected | Privacy Policy | FTC en español

Search

ABOUT THE FTC NEWS & EVENTS ENFORCEMENT POLICY TIPS & ADVICE I WOULD LIKE TO...

Home » Enforcement » Statutes » Federal Trade Commission Act

Federal Trade Commission Act

TAGS: Competition | Consumer Protection | Alcohol | Appliances | Automobiles | Clothing and Textiles | Finance | Franchises, Business Opportunities, and Investments | Funerals | Jewelry | Real Estate and Mortgages | Tobacco | Advertising and Marketing | Advertising and Marketing Basics | Children | Endorsements | Environmental Marketing | Health Claims | Made in USA | Online Advertising and Marketing | Telemarketing | Credit and Finance | Credit and Loans | Debt | Debt Collection | Mortgages | Payments and Billing | Privacy and Security | Children's Privacy | Consumer Privacy | Credit Reporting | Data Security | Gramm-Leach-Bliley Act | Red Flags Rule

MISSION: Competition | Consumer Protection

HHS.gov U.S. Department of Health & Human Services

Health Information Privacy

I'm looking for...

HHS A-Z Index

HIPAA for Individuals Filing a Complaint HIPAA for Professionals Newsroom

HHS Home > HIPAA > HIPAA for Professionals

HIPAA for Professionals

Text Resize A A A Print Share

HIPAA for Professionals

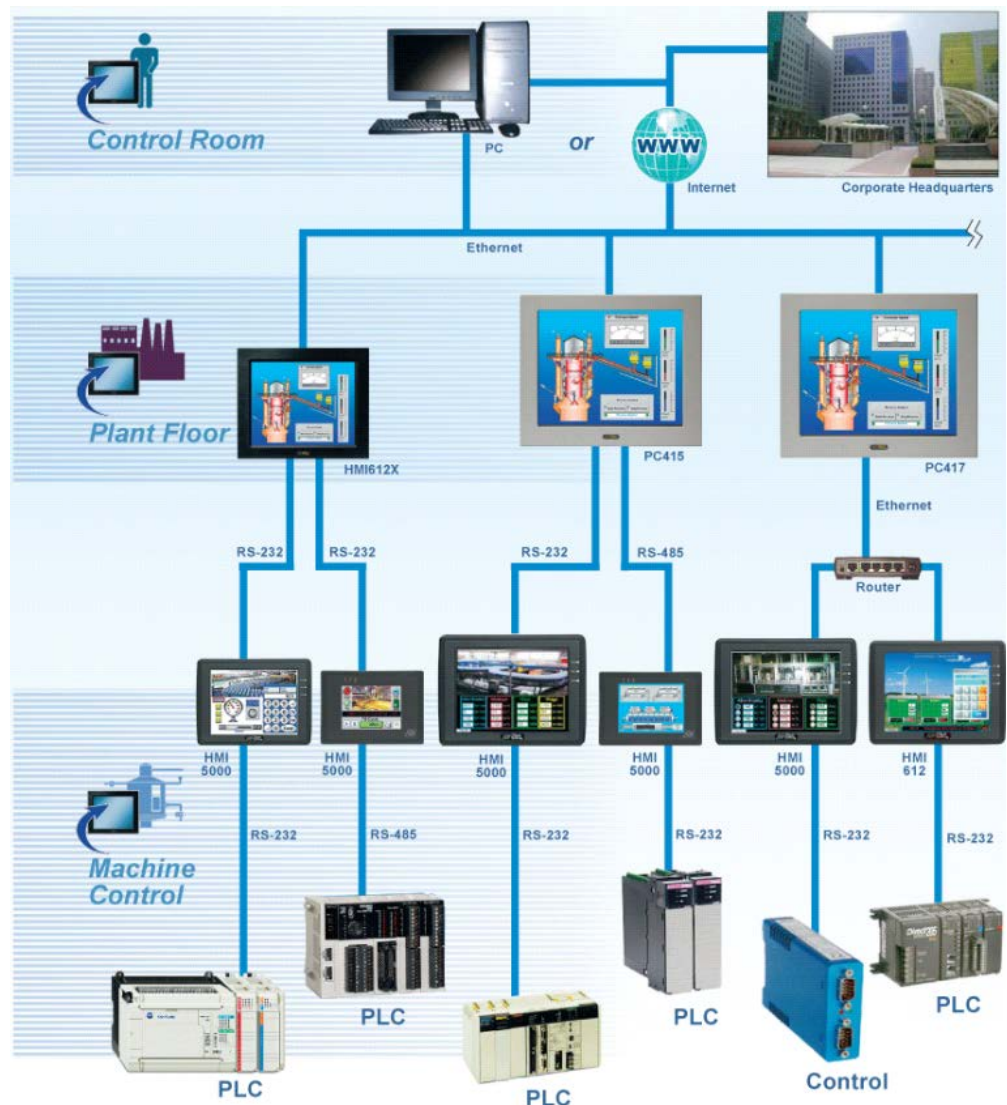
To improve the efficiency and effectiveness of the health care system, the [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

- HHS published a final [Privacy Rule](#) in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- HHS published a final [Security Rule](#) in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).
- The [Enforcement Rule](#) provides standards for the enforcement of all the Administrative Simplification Rules.
- HHS enacted a [final Omnibus rule](#) that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA.

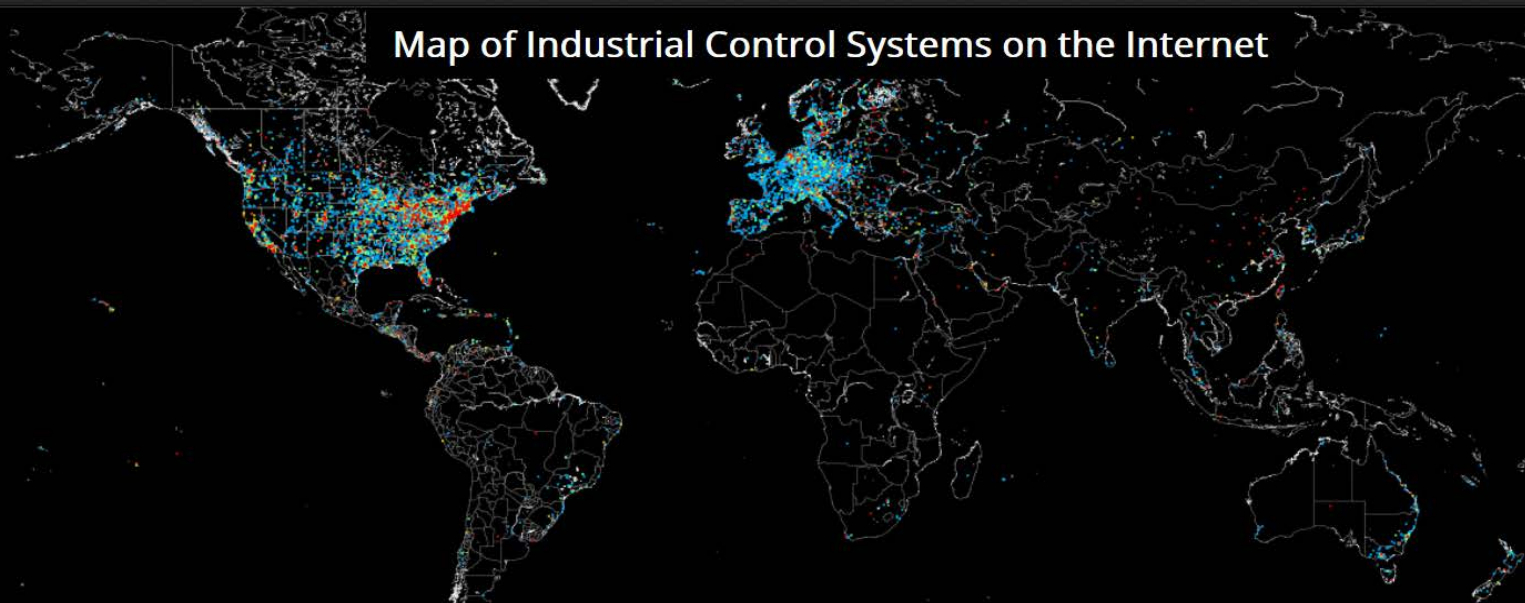
From hardwired “island operation” to a interconnected ICS networks

THE PAST: HARDWIRED INTERFACES

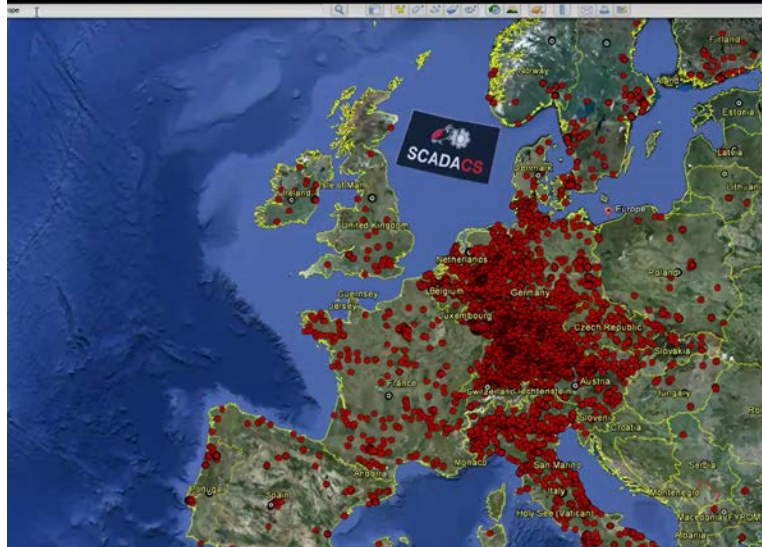
- ▶ A collection of **dry contact** inputs/outputs were used to fulfill a **correlation matrix** to meet a specific project integration objective
- ▶ **Relay Logic** was used to design complex interfaces
- ▶ Systems were poorly documented if at all and **nearly impossible to maintain or extend**



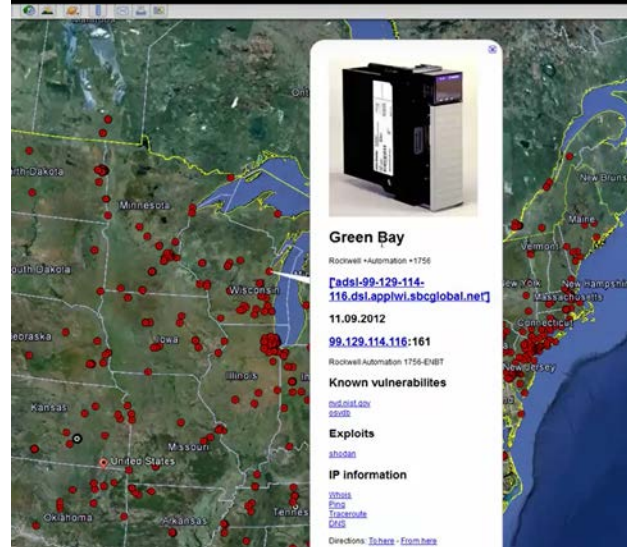
Map of Industrial Control Systems on the Internet



IRAM Industrial Risk Assessment Map by SCADACS www scadacs org



www scadacs org



➤ IoT & ICS search engines

ExO 13636 – US Gov recommendations - incentives for cyber insurance



Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Department of Homeland Security
Integrated Task Force

Incentives Study Analytic Report

June 12, 2013



**Homeland
Security**

- Implementation of cybersecurity practices & standards
- Increase of cyber information sharing
- Develop awareness for cyber aspects of how infrastructure functions
- Understand cascading of infrastructure failures

https://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Discussion_Final.pdf

<https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

https://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf

<http://www.bna.com/the-potential-effect-of-executive-order-13636-on-cybersecurity-insurance-coverage/>

<https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf>

NIS Directive- incentives for cyber insurance



The screenshot shows the European Commission website page for the Network and Information Security Directive. The page is titled "DIGITAL SINGLE MARKET Digital Economy & Society". The main heading is "Network and Information Security Directive: co-legislators agree on the first EU-wide legislation on cybersecurity". The page is published on 09/12/2015. The content includes a summary of the agreement reached on 7th December 2015, and a list of key features of the new rules, such as improving cybersecurity capabilities, cooperation, and requiring operators of essential services to take appropriate security measures and report incidents to national authorities.

European Commission > Network and Information Security Directive: co-legislators agree on the first EU-wide legislation on cybersecurity

Society

Skills & Jobs

eHealth and Ageing

Smart living

Digital Inclusion

Public Services

Cybersecurity and privacy

Cybersecurity

Cybersecurity industry

Online privacy

EU Funded Projects

Online trust

Content and media

Emergency and support lines

Societal challenges projects

Network and Information Security Directive: co-legislators agree on the first EU-wide legislation on cybersecurity

Published on 09/12/2015

On 7th December 2015, the European Parliament and the Council reached an agreement on the Commission's proposed measures to increase online security in the EU. The Network and Information Security (NIS) Directive is the first piece of European legislation on cybersecurity. Its provisions aim to make the online environment more trustworthy and, thus, to support the smooth functioning of the EU Digital Single Market.

The proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union was put forward by the European Commission in 2013. Two years later, the Parliament and the Council have agreed on a set of measures to boost the overall level of cybersecurity in the EU.

The new rules will:

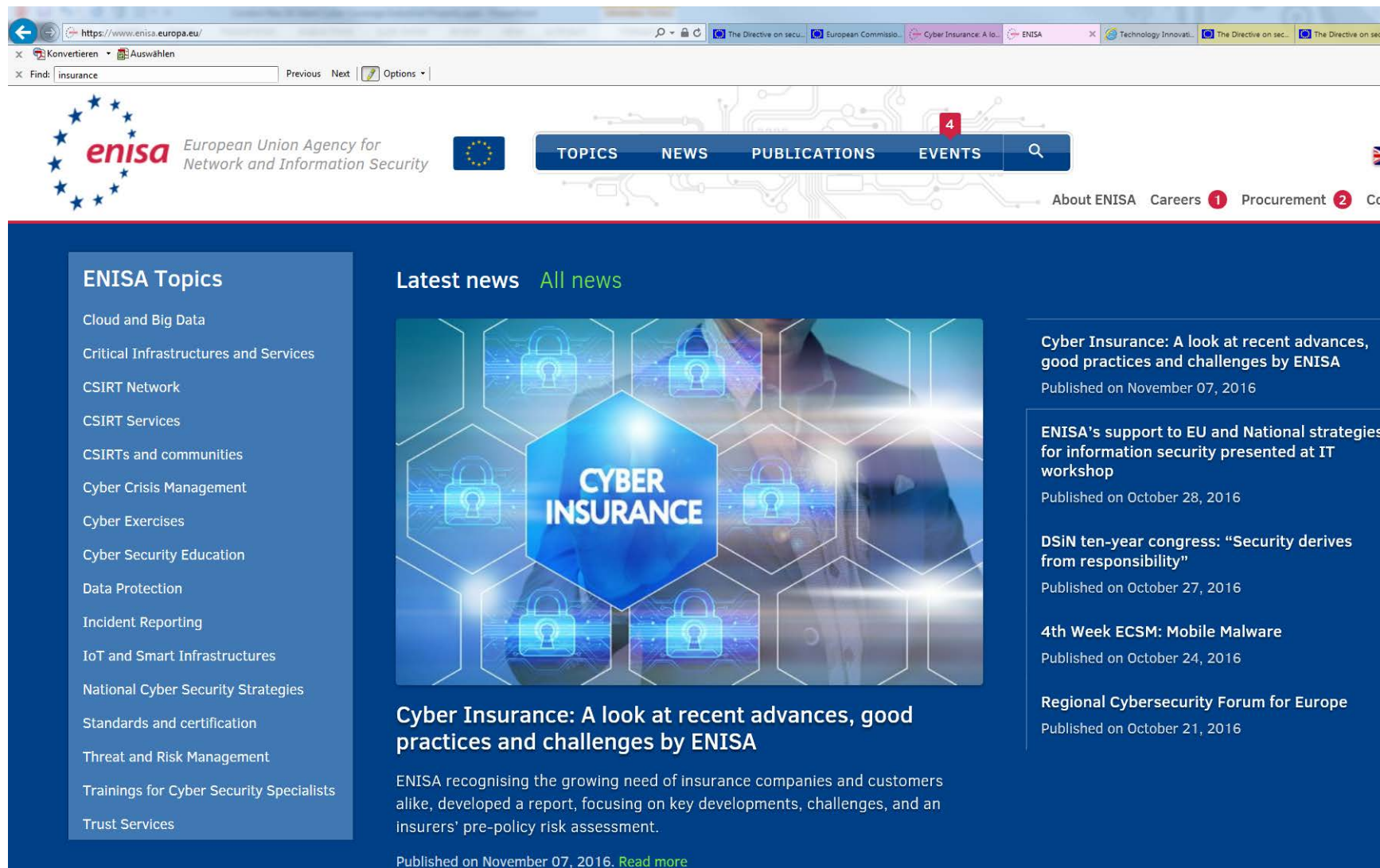
- improve **cybersecurity capabilities** in Member States
- improve Member States' **cooperation** on cybersecurity
- require **operators of essential services** in the energy, transport, banking and healthcare sectors, and providers of key digital services like search engines and cloud computing, **to take appropriate security measures and report incidents to the national authorities.**

Share

Europ. Commission Vice-President: "people & businesses ... need to trust ... in secure online environment and ... use digital tools, networks and services in the EU with confidence. The NIS Directive is the EU legislation on cybersecurity... & requires companies in critical sectors ... to adopt risk management practices and report major incidents to their national authorities..."

- **Entry in force August 2016**
- **Transposition into national law May 2018**

ENISA leads NIS development and implementation of the European Union's policy and law



The screenshot shows the ENISA website interface. At the top, there is a navigation bar with the ENISA logo and the text "European Union Agency for Network and Information Security". The navigation menu includes "TOPICS", "NEWS", "PUBLICATIONS", and "EVENTS". Below the navigation bar, there is a search bar and a list of links: "About ENISA", "Careers", "Procurement", and "Cc".

The main content area is divided into two columns. The left column is titled "ENISA Topics" and lists various categories such as "Cloud and Big Data", "Critical Infrastructures and Services", "CSIRT Network", "CSIRT Services", "CSIRTs and communities", "Cyber Crisis Management", "Cyber Exercises", "Cyber Security Education", "Data Protection", "Incident Reporting", "IoT and Smart Infrastructures", "National Cyber Security Strategies", "Standards and certification", "Threat and Risk Management", "Trainings for Cyber Security Specialists", and "Trust Services".

The right column features a "Latest news" section with a link to "All news". The main article is titled "Cyber Insurance: A look at recent advances, good practices and challenges by ENISA". The article text reads: "ENISA recognising the growing need of insurance companies and customers alike, developed a report, focusing on key developments, challenges, and an insurers' pre-policy risk assessment." The article is published on November 07, 2016, and includes a "Read more" link.

Below the main article, there is a list of other news items:

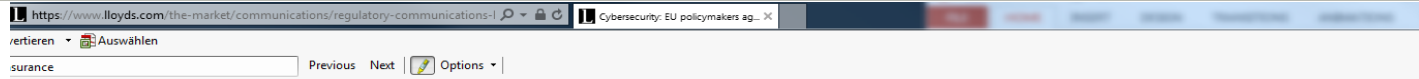
- Cyber Insurance: A look at recent advances, good practices and challenges by ENISA**
Published on November 07, 2016
- ENISA's support to EU and National strategies for information security presented at IT workshop**
Published on October 28, 2016
- DSiN ten-year congress: "Security derives from responsibility"**
Published on October 27, 2016
- 4th Week ECSM: Mobile Malware**
Published on October 24, 2016
- Regional Cybersecurity Forum for Europe**
Published on October 21, 2016

NIS – safe networks for critical services

Essential Services in Critical Sectors	Energy (Electricity, Oil, Gas)
	Transport (Air transport, Rail transport, Water transport, Road transport)
	Banking
	Financial market infrastructures
	Health sector
	Drinking water supply and distribution
	Digital Infrastructure
Digital Service Providers	Online marketplace
	Online search engine
	Cloud computing service

Table 1: Types of entities for the purposes of point (4) of Article 4 of NIS Directive

Lloyds position on NIS



Key points

- **Application** - The NIS Directive imposes obligations on operators of essential services and providers of key digital services and lists the essential services to which it applies. This list includes, among other sectors, transport, banking, financial market infrastructures, healthcare and energy. It does not mention insurers explicitly.
- **Minimum harmonisation** - The Directive sets out minimum harmonisation measures and Member States are not prevented from adopting more restrictive provisions to achieve higher levels of NIS security. In the implementation phase, it is for Member States to identify specific entities, under each sector listed, to which the rules will apply.
- **Increased national cybersecurity capabilities** - Each EU Member State must adopt a national strategy and appropriate cybersecurity measures. They must establish a National Competent Authority (NCA) to monitor implementation of the rules, as well as Computer Security Incident Response Teams responsible for handling incidents.
- **Security and notification requirements** - The businesses to which the Directive is applied will have to take appropriate security measures to manage the risks posed to the network and information systems they control and use in their operations. They will be required to notify to the relevant NCA, without undue delay, incidents having a significant impact on the continuity of the core services they provide.
- **Cooperation network** - The EU Commission and the NCAs will form a cooperation network tasked with supporting and facilitating strategic cooperation and exchange of information.
- **Sanctions** - Breach of the obligations imposed by the Directive may attract onerous administrative sanctions. It is the responsibility of Member States to determine penalties which, according to the Directive, must be "effective, proportionate and dissuasive".

Interplay between NIS Directive and EU General Data Protection Regulation ("GDPR")

Although both the NIS Directive and the [GDPR laws](#) impose requirements on operators to adopt risk-based security measures as well as mandatory incident notification in case of breaches, they protect different interests and may apply to distinct types of incidents.

Whilst the [GDPR aims to safeguard personal data](#), the [Directive's focus is on network security](#). The targets are also distinct: where the GDPR will apply to any person or entity involved in the processing of personal data of individuals in the EU, the NIS Directive is addressed to operators of essential services and digital service providers.

Finally, the NIS Directive does specify that, in cases where personal data are compromised as a result of serious incidents, NCAs and data protection authorities must cooperate and exchange all relevant information to address personal data breaches resulting from incidents.

Impact on the Lloyd's market

- *Risk management implications* - Although insurers are out of the scope of the Directive, the final decision on whether certain entities meet the Directive's criteria will be remitted to Member States.
- Financial market infrastructures and banks will be subject to breach reporting obligations and minimum security requirements. In the implementation phase, if the UK extends the obligation to meet cyber security requirements to all financial services firms, Lloyd's managing agents and intermediaries will need to comply with the rules.
- *Impact on underwriting* - Lloyd's remains a market leader in cyber insurance. Once implemented, the NIS Directive may drive demand for cyber insurance in Europe.
- The new EU rules support the creation of a risk management culture and will improve information sharing practices between the private and public sectors. This will help underwriters to analyse rapidly-evolving cyber threats and risk managers to reduce uncertainty and address better solutions.

Next steps

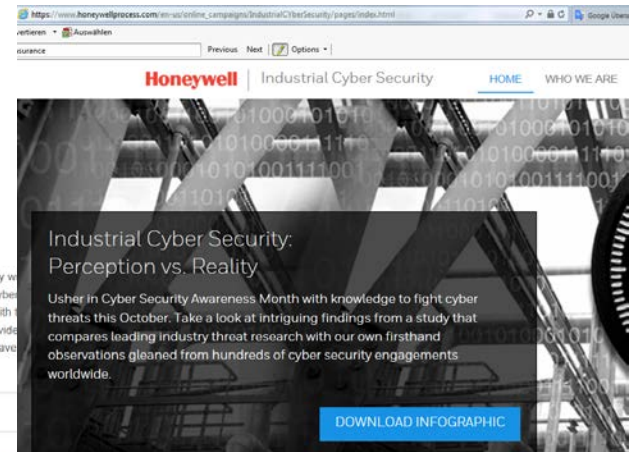
The political agreement reached in December 2015 needs to be formally adopted by the European Parliament and the EU Council (expected in spring 2016). Once published in the EU Official Journal, Member States will have 21 months to implement the NIS Directive into national law and a further six months to identify operators of essential services.

Industry geared up



Cyber threats

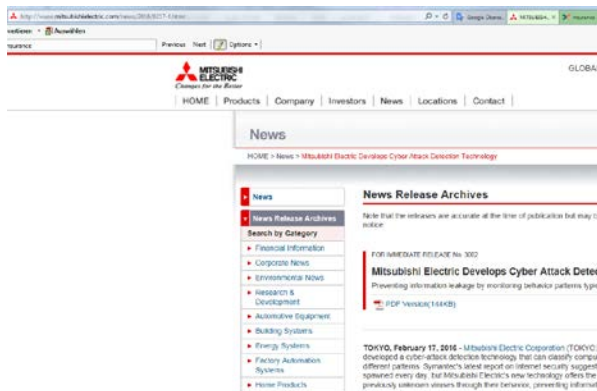
Cyber attacks present a risk to the security of our information, IT systems and operations. We collaborate closely with governments, law enforcement agencies and industry peers to understand and respond to new and emerging cyber threats. We also monitor our IT systems for suspicious activity and have a 24-hour monitoring centre in the US tasked with promoting good cyber security behaviours in our workforce through easy-to-understand policies and instructional videos. Campaigns and presentations on topics such as email phishing and protecting our information and equipment have raised employee awareness of these issues.



Industrial Cyber Security: Perception vs. Reality

Usher in Cyber Security Awareness Month with knowledge to fight cyber threats this October. Take a look at intriguing findings from a study that compares leading industry threat research with our own firsthand observations gleaned from hundreds of cyber security engagements worldwide.

DOWNLOAD INFOGRAPHIC

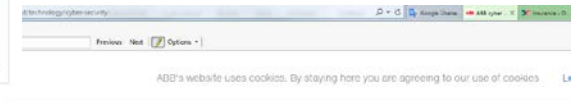


Q: How big a risk is cybersecurity for BP?

A: News headlines frequently contain reports of cyber attacks stealing huge volumes of information or, increasingly, causing damage and disrupting business operations. These events have demonstrated how quickly systems once believed to be secure can become vulnerable. This complex, fast-changing landscape, and BP's reliance on technology, mean that cybersecurity is a risk BP takes very seriously. Cybersecurity is one of the company's highest level risks and is monitored by the board. We take an intelligence-led approach to evolve our cyber defences and response, in line with the fast-changing threats.



Daniel Barriuso, chief information security officer, BP



Cyber security

Integrated, customer-oriented cyber protection



ABB works closely with customers to create a defense in depth approach to cyber security.



Home > About Yokogawa > News > 2015 Press Releases > Press Release - February 10, 2015

Press Release - February 10, 2015

Tokyo, Japan - February 10, 2015

Yokogawa and Cisco Deliver Cybersecurity Solutions for Shell

Let's have a look now on Insurance

- Legislator did their homework
- Industry did their homework

Onus of proof & ambiguities in current wording

❑ Policy holder: ... demonstrates «claim triggers policy»

❑ Insurance: ... demonstrates «exclusion applies»

- CL / NMA clauses not stress tested – no court decisions regarding cyber induced PD / BI
- Terms not specified
- Complex clauses

Institute Cyber Attack Exclusion Clause (CL 380), 10/11/03

1. Subject only to clause 1.2 below, **in no case shall this insurance cover loss** damage liability or expense directly or indirectly caused by or contributed to by or arising **from the use** or operation, **as a means for inflicting harm, of any** computer, **computer system**, computer software programme malicious code, computer virus or process or any other electronic system.
2. Where this Clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1. Shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system computer software programme, or any electronic system in the launch and/o guidance system and/or firing mechanism of any weapon or missile.

... in no case shall this insurance cover loss ... from the use ... - as a means for inflicting harm - of any computer system...

➤ ask IT forensics about intention / inadvertent ...

Cyber Non-Aggregation Clause (NMA 2912) – IT Hazards Exclusion Clause (NMA 2928)

Losses arising, directly or indirectly, **out of** :

i. loss of, alteration of, or **damage** to

or

ii. a **reduction in the functionality**, availability or operation **of**

a computer system, hardware, programme, software, data information repository, microchip, integrated circuit or similar device in computer equipment or non-computer equipment, whether the property of the policyholder of the reinsured or not, **do not** in and of themselves **constitute an event unless arising out of** one or more of the following perils:

Fire, lightning, explosion, aircraft or vehicle impact, falling objects, windstorm, hail, tornado, cyclone, hurricane, earthquake, volcano, tsunami, flood freeze or weight of snow.

... losses out of damage or reduction in the functionality of a computer system do not constitute an event unless arising out of FLEXA and/or Natural Hazards...

➤ FLEXA causes ICS disruption **OR** ICS disruption causes FLEXA ???
Good luck in court **AND** if you have to explain to policy holder ...

Electronic Data Endorsement A (NMA 2914), 25/01/2001

1. Electronic Data Exclusion

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

- a) This Policy does **not insure**, loss, damage, destruction, distortion, erasure, corruption or alteration of **ELECTRONIC DATA** from any cause whatsoever (including but not limited to COMPUTER VIRUS) **or loss of** use, reduction in **functionality**, cost, expense of whatsoever nature **resulting therefrom**, regardless of any other cause or event contributing concurrently or in any other sequence to the loss.

ELECTRONIC DATA means facts, concepts and information converted to a form useable for communications, interpretation or processing by electronic and electromechanical data processing or electronically controlled equipment and includes programmes, software, and other coded instructions for the processing and manipulation of data or the direction and manipulation of such equipment.

COMPUTER VIRUS means a set of corrupting, harmful or otherwise unauthorised instructions or code including a set of maliciously introduced unauthorised instructions or code, programmatic or otherwise, that propagate themselves through a computer system or network of whatsoever nature. COMPUTER VIRUS includes but is not limited to 'Trojan Horses', 'worms' and 'time or logic bombs'.

... ELECTRONIC DATA not insured ...

Electronic Data Endorsement A (NMA 2914), 25/01/2001

b) However, in the event that a **peril listed below results from any of the matters described in paragraph a)** above, this Policy, subject to all its terms, conditions and exclusions **will cover physical damage** occurring during the Policy period to property insured by this Policy directly caused by such listed peril.

Listed Perils: **Fire, Explosion**

2. Electronic Data Processing Media Valuation

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

Should electronic data processing media insured by this Policy suffer physical loss or damage insured by this Policy, then the basis of valuation shall be the cost to repair, replace or restore such media to the condition that existed immediately prior to such loss or damage, including the cost of reproducing any ELECTRONIC DATA contained thereon, providing such media is repaired, replaced or restored. Such cost of reproduction shall include all reasonable and necessary amounts, not to exceed [Response] any one loss, incurred by the Assured in recreating, gathering and assembling such ELECTRONIC DATA. If the media is not repaired, replaced or restored the basis of valuation shall be the cost of the blank media. However this Policy does not insure any amount pertaining to the value of such ELECTRONIC DATA to the Assured or any other party, even if such ELECTRONIC DATA cannot be recreated, gathered or assembled.

[PD caused by] Fire, Explosion resulting from loss of functionality or loss of ELECTRONIC DATA will be covered ...

CL 380 exchanged for NMA 2914/5

“In no case shall this insurance cover loss from the use - as a means for inflicting harm - of any computer system”

FOR

“PD caused by Fire, Explosion resulting from loss of (ICT) functionality or loss of ELECTRONIC DATA will be covered “

NMA 2912/28 exchanged for NMA 2914/5

“... losses out of damage or reduction in the functionality of a computer system do not constitute an event unless arising out of FLEXA and/or Natural Hazards...”

FOR

“PD caused by Fire, Explosion resulting from loss of (ICT) functionality or loss of ELECTRONIC DATA will be covered “

UW considerations – intended vs. inadvertent – cyber war – cyber terror

- Cyber incidents are not always intended
 - wrong coding
 - wrong interaction of two control units
 - manual bypass of alarm management system during commissioning

→ effect could be equal to an malicious attack

- Targeted cyber incidents are not sudden and unforeseen
 - initial attack/infection could even have happened before the policy inception
- Targeted cyber attacks can produce losses higher than PML assessed

- Motivation of a cyber attack can be different – but method of a cyber attack and resulting damage are of the same kind
 - to distinguish between war, terror, sabotage, malicious act is **pointless**

Conclusion

- Under current (outdated?) market wordings ...
 - we should assume, that we cover cyber

- As attack surface & exposure changed, we cover the PD component of cyber & should get premium for it
 - on the Brick Lane you never get a curry for free despite the overcapacity

- If one wants to exclude it:
 - use clear wording and assume the consequences
 - i.e. onus of proof that an exclusion applies
 - network forensics \$700/h p.c. (2 weeks presence of 2 specialists = \$120k)

Q & A ?

Panel Discussion

IMIA Draft Advanced Cyber Exclusion Clause



ZURICH®

Participants

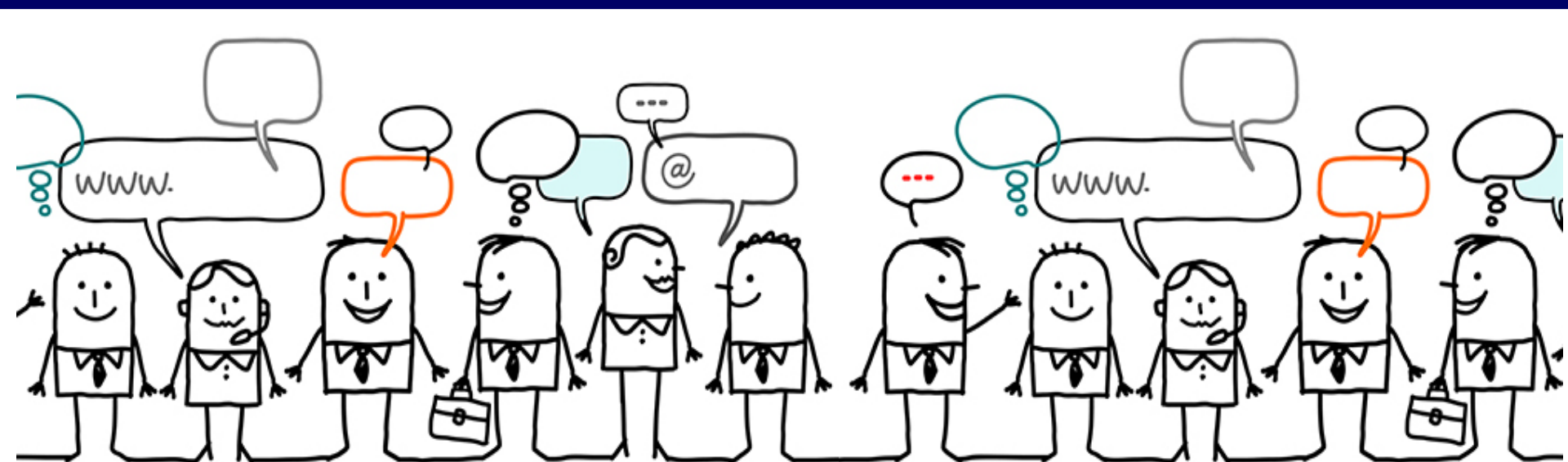
Paul Lowrie, Partner - Clyde & Co LLP

Aiko Schilling, Senior In-House Counsel Wordings - Munich Re

Andrew Herring, Practice Leader Energy EMEA region - Marsh

Israel Silverman, Vice President Associate General Counsel - SCOR

Markus Bassler, Head of Energy Onshore & Special Risks - Partner Re





IMIA

Advanced Cyber Exclusion Endorsement

London, 16th of November, 2016

Dr. Aiko Schilling

Initial Status (1)

All Cyber Exclusions on the marked have some weaknesses:

- **CL380:**

“...caused by or contributed to by or arising from the use or operation, as a MEANS for INFLICTING HARM...” → subjective requirement which could cause discussions after a loss!
- **NMA 2914/15:**

“However, in the event that a peril listed below...will cover PHYSICAL DAMAGE...”
→ Is this a physical damage trigger for the Business Interruption respectively DSU/Alop Section?
- **NMA 2912/28:**

“Losses arising...out of...unless arising out of one or more of the following perils:..”
→ What shall happen in case of a loss of Data caused by the named perils? Unlimited coverage?
Also for the value of the Data? What does mean „Losses“? Also/only Business Interruption?

Initial Status (2)

...and there are further Open Questions with regard to these Cyber Exclusions:

- Do we need better Definitions for some cyber-related terms used in these Exclusions?
- How to interpret some oldfashioned terms and to use them for today's OT and IT landscape?
- Are Data Insured Property?
- How to deal with the Burden of Proof?
- What about Cyber Extortion?
- What about new Cyber Threats such as System Failure, Human Error or a Rogue Employee?
- What about Cyber Claims Management Processes?

IMIA

Advanced Cyber Exclusion Endorsement

- Providing the possibility to manage consciously (NOT only exclude!) cyber cover within engineering and other covers.
- Comprehensive Wording answers most of the mentioned Open Questions and tries to avoid the weaknesses of the existing Exclusions
- Provision of Definitions for the cyber-related Technical Terms
- Right of the (Re)Insurer to send Experts to the site of the Insured conducting Forensic Investigations
- Making Underwriters aware of the fact that „Cyber“ is a complex topic with different Exposures
- Providing Transparency for the Underwriters regarding additional Exposure and Risk Return regardless of the market environment

IMIA Advanced Cyber Exclusion Endorsement with Controlled Writ-back Option

Due to the fact that the IMIA Advanced Cyber Exclusion Endorsement creates an absolute Cyber Exclusion Underwriters are able to offer to the Insureds an individual and tailor-made Write-back for specific Cyber Risks:

Write-back Endorsement – 2016 – NMA 2914/15 (Draft)

Endorsement forms part of Policy No.:xxxxxx

Issued to:

Issued by:

Effective:

Endorsment No.:

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

This Policy shall - subject to all its terms, conditions and exclusions - cover physical damage occurring during the Policy Period to property insured (**including any insured business interruption losses resulting therefrom**) in the event that a peril listed below results from a cyber incident as set forth in provision **a), b), c), d), e), f)** of Clause 1 of the Advanced Cyber Exclusion 2016.

Listed Perils: **Fire, Explosion**

All other terms and conditions remain unchanged.

Panel Discussion



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:

Conclusions

Workshop Closing

