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

Evolution of the Mobile Phone

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

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

26 Billion installed units by 2020

Device Categories

Future DDoS Attacks Could Reach 10 Tbps
EU & US - Protection of personal data

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.

GDPR Portal: Site Overview

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

FEDERAL TRADE COMMISSION

Protecting America’s Consumers

Federal Trade Commission Act

Home » Enforcement » Statistics » Federal Trade Commission Act


MISSION: Competition | Consumer Protection

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, 2002 (April 14, 2003, 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.

[Diagram of interconnected ICS networks]

https://en.wikipedia.org/wiki/SCADA
IoT & ICS search engines
And how are vulnerabilities exploited?
see German Federal Office for Information Security (BSI) – Report 2014

https://www.youtube.com/watch?v=OVMwI2TwZw
ExO 13636 – US Gov recommendations - incentives for cyber insurance

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

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
## NIS – safe networks for critical services

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

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 the event 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**: They will be subject to breach reporting obligations and minimum security requirements. In the implementation phase, if the UK extends the obligation to meet cybersecurity 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.

- **New EU rules support**: 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 behaviour 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 computer hardware raise employee awareness of these issues.

Cybersecurity

Comprehensive cyber protection
Combining “Defense in Depth” with lifecycle activities

Cybersecurity

Cyber threats

Cybersecurity

Integrated, customer-oriented cyber protection


Yokogawa and Cisco Deliver Cybersecurity Solutions for Shell

Cybersecurity

Cyber threats

Cybersecurity

Comprehensive cyber protection
Combining “Defense in Depth” with lifecycle activities

Cybersecurity

Integrated, customer-oriented cyber protection


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 ...
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 a 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 ?