Swiss Re

Maritime Insurance Cyber Security – Framing the Exposure

Tony Cowie – May 2015

Table of Contents / Agenda

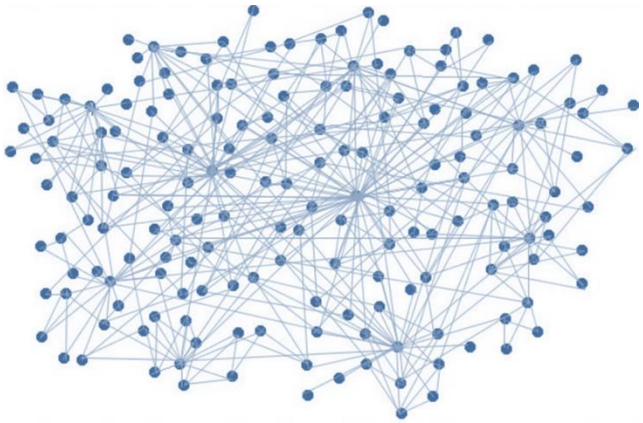
- What is cyber risk?
- Exposures - Should we be concerned about "Cyber"?
- Is Cyber covered under a Marine Insurance Policy? What about a Reinsurance Treaty?
- How is the maritime insurance industry currently addressing the situation?
- Further Reading / Insurance Market in Cyber /How can insurers increase Cyber Risk Resilience?

What is cyber risk?

CYBER RISK – covers the risks of doing business, including managing and controlling data, in a digital or "cyber" environment

Factors influencing the threat landscape

- The Cloud
- Shadow IT
- Mobile and flexible working
- Bring your own devices
- Internet of things



Sources

- Human/ system error
- Cyber crime
- Lone hackers
- State-backed

Tools and expertise needed to exploit vulnerabilities are becoming more widely available

Ability to carry out an attack is therefore simpler

Should we Mariners be concerned about "Cyber"?

- University of Texas researchers demonstrated in July 2013 that it is possible to change a vessel's direction by interfering with its GPS signal to cause the onboard navigation systems to falsely interpret a vessel's position and heading
- Hacker caused a floating oil platform off Africa to tilt to one side, forcing temporary shutdown. *(Note this story is all over the internet, and in the IMO report, but I was unable to verify the actual platform)*
- Somali pirates employed hackers to infiltrate a shipping company's cyber systems to identify vessels passing through the Gulf of Aden with valuable cargoes and minimal on-board security which led to the hijacking of at least one vessel

All examples from a report submitted by Canada to the IMO in July 2014 (http://www.protect-group.org/assets/Uploads/FAL-39-7-Measures-toward-enhancing-maritime-cybersecurity-Canada.pdf)

Should we Mariners be concerned about "Cyber"?

- Denial of service attacks (initiating a very high number of requests to a system to overwhelm it and cause it to cease operating) against ports have been reported *(Houston being one of them)*
- Efforts to gain unauthorized access to wireless Internet networks in ports have been reported
- Studies by the Brookings Institute and the European Union Agency for Network and Information Security both concluded that *there is very little awareness of cybersecurity issues in the maritime transportation sector and few initiatives underway to enhance cybersecurity*.

All examples from a report submitted by Canada to the IMO in July 2014 (http://www.protect-group.org/assets/Uploads/FAL-39-7-Measures-toward-enhancing-maritime-cybersecurity-Canada.pdf)

Should we Mariners be concerned about "Cyber"?

Lot of reports of stolen or corrupted data, but any physical losses?

Cyberattack on German Iron Plant Causes 'Widespread Damage': Report

Rachael King

Dow Jones Institutional News

A German federal agency has acknowledged in a report Wednesday that a cyberattack caused physical damage to an iron plant in the country. It was a rare admission by a government tying a cyber action to actual physical destruction.

The attackers gained access to an unnamed plant's office network through a targeted malicious email and were ultimately able to cross over into the production network. The plant's control systems were breached which "resulted in an incident where a furnace could not be shut down in the regular way and the furnace was in an undefined condition which resulted in massive damage to the whole system," according to the report, called the IT Security Situation in Germany in 2014.

"**I know of seven other incidents that have claimed to have had a cyber-to-physical or significant process effect and a few near misses that were caught in time," said Michael Assante industrial control systems lead for SANS Institute, a cybersecurity research and education organization**, in an email.

"The industrial control systems community is very secretive for legal and compliance reasons," Mr. Lee told CIO Journal. However, he sees Germany's acknowledgement of the attack on the plant as a sign that things are starting to change. "We're absolutely reaching a point where it's becoming more normal and expected to talk about these things rather than run from them," he said.

- From 18 Dec 2014 Wall Street Journal

- I could not find any reports of Marine Physical Loss

Should we Mariners be concerned about "Cyber"?

YES

- We certainly have potential exposure here.
- Experts estimate that **hacking attacks** against gas and oil infrastructures will cost energy companies upwards of $2 billion by the time 2018 rolls around.
  (note it is unclear if this is in expected losses or additional expenses to combat the exposure – US Gov't currently spending circa $10B a year on Cyber Risk)
- I could find no estimates on the potential economic impact to the Hull and Cargo sectors – does not mean it is not there.

Is Cyber covered under a Marine Insurance Policy? What about a Reinsurance Treaty?

- Maybe
  - Marine / Energy Insurance Policies are so varied and/or bespoke, hard to give a definite answer, but assuming an "all risk policy" without a proper exclusion, then I would say yes, cover would be found for a "Cyber" loss. Read your policy!
  - Marine / Energy Reinsurance Treaty may or may not include exclusionary and / or non accumulation language. Reinsurers may rely on a warranty from the Primary Insurer to apply exclusionary language on each and every original policy.
- Is cyber crime just good old-fashioned crime like theft, vandalism, fraud and kidnap, but perpetrated in "cyberspace", using computer code over the internet? How is it different from conventional crime? The greater distance and time between the criminal and the crime? The scale of the proceeds of the crime in terms of volume and value? The manner in which the consequences can cascade across enterprises and market sectors?

Something to think about


Thank You for Your Kind Attention

Further Reading

- Canada Cyber Report to the IMO - July 2014 (http://www.protect-group.org/assets/Uploads/FAL-39-7-Measures-toward-enhancing-maritime-cybersecurity-Canada.pdf
- **Cyber Resilience - the cyber risk challenge and the role of insurance http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/**
- **Ideas for** Resilience

Insurance Market in Cyber

Insurance is increasingly part of the strategy to manage cyber risk

Market for insurance products specifically designed to cover cyber risk is expected to continue to evolve in response to:

- Increased publicity around breaches which reinforces the potential economic impact of a cyber attack
- High profile court rulings (Zurich America Insurance Co. vs. Sony Corp of America et al).
- Regulatory shifts in the US (SEC guidance) and in the EU (Data protection regulation)
- Changes in policy language (e.g. Insurance Services Office (ISO) standard exclusion for cyber risk under the commercial general liability policy)
- Government initiatives such as the UK's Cyber Essentials Scheme and the US NIST framework

However, there continue to be challenges to an insurance market for cyber risk due to:

- Continually shifting threats
- Sparse loss data
- Increasing complexity and interconnectivity

A well-functioning insurance market for cyber risk requires appropriate risk management

Common classification and codification of cyber risks and **understanding of cyber risk exposure accumulation** are pre-requisites to a **strong and well designed risk management framework**

How can insurers increase Cyber Risk Resilience?

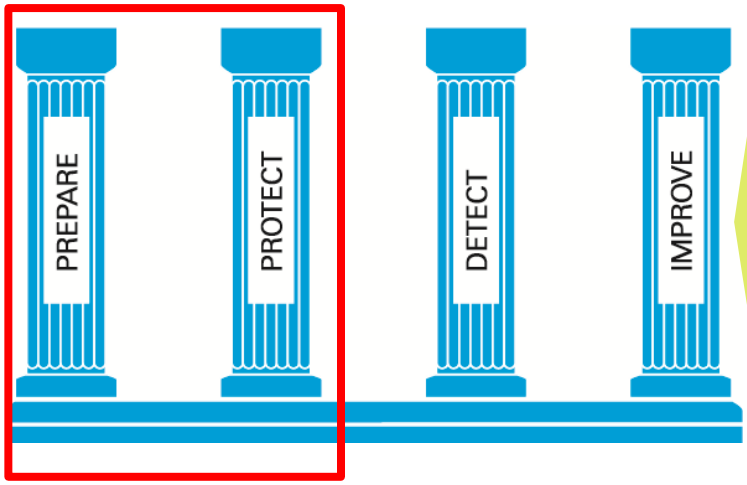
PREPARE

Understand your critical assets (data and systems)
- ❑ What is vital to protect?

Develop capabilities to address different levels of risk
- ❑ New approaches to assurance and threat management
- ❑ Build good relationships with industry and government

Establish risk appetite
- ❑ Understand regulatory, environmental and operational requirements
- ❑ Risk tolerance

Embed cyber risk management throughout the organisation



PROTECT

Ensure well founded and repeatable cyber preparedness
- ❑ Strong levels of IT hygiene

Undertake Threat and Control Assessments
- ❑ Understand cyber threat landscape

Ensure appropriate due diligence and vetting of third parties

Enable and empower incident management and response capabilities

Develop and implement an incident response plan

Education and training
- ❑ Cyber risk understanding and awareness

Historically, there has been too much focus on **PREPARE** and **PROTECT** and insufficient focus on **DETECT** and **IMPROVE**

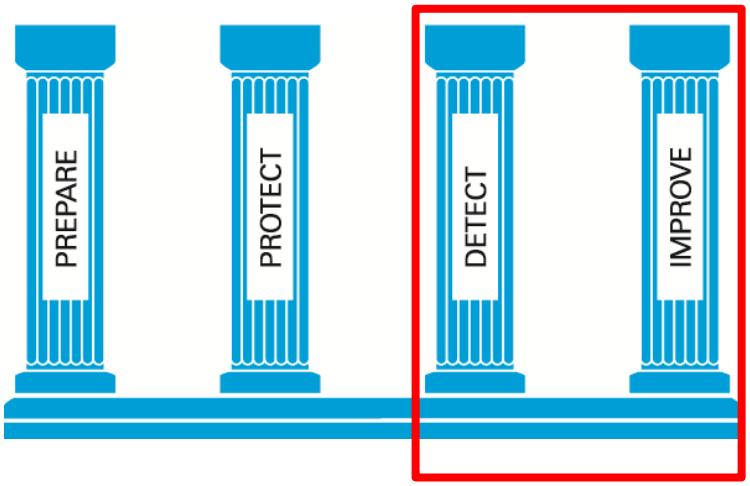
How Can Insurers Increase Cyber Risk Resilience?

DETECT

Develop detection and continuous monitoring

- ❑ Continuous monitoring to detect anomalies and threats
- ❑ Incident response teams
- ❑ Regular testing of detection capabilities

UK government estimates indicate that, on average, **200** days elapse between the occurrence of a security incident and its detection



IMPROVE

Build a comprehensive database of security incidents

- ❑ Include near miss/ minor events
- ❑ Capture lessons learnt to allow ongoing modification/ improvement

Recover from an event

- ❑ Execute the recovery plan
- ❑ Learn from experience to allow ongoing modification/ improvement

Legal notice

The information and opinions contained in the presentation are provided as at the date of the presentation and are subject to change without notice. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the details given. All liability for the accuracy and completeness thereof or for any damage or loss resulting from the use of the information contained in this presentation is expressly excluded. Under no circumstances shall Swiss Re or its Group companies be liable for any financial or consequential loss relating to this presentation.