Image: Munich Re Oliver Soulas

Maritime Cyber Risks

Aqaba Conference 11.05.2015 – 13.05.2015

Alexander Kababgi, Claims Manager

Munich RE

Agenda

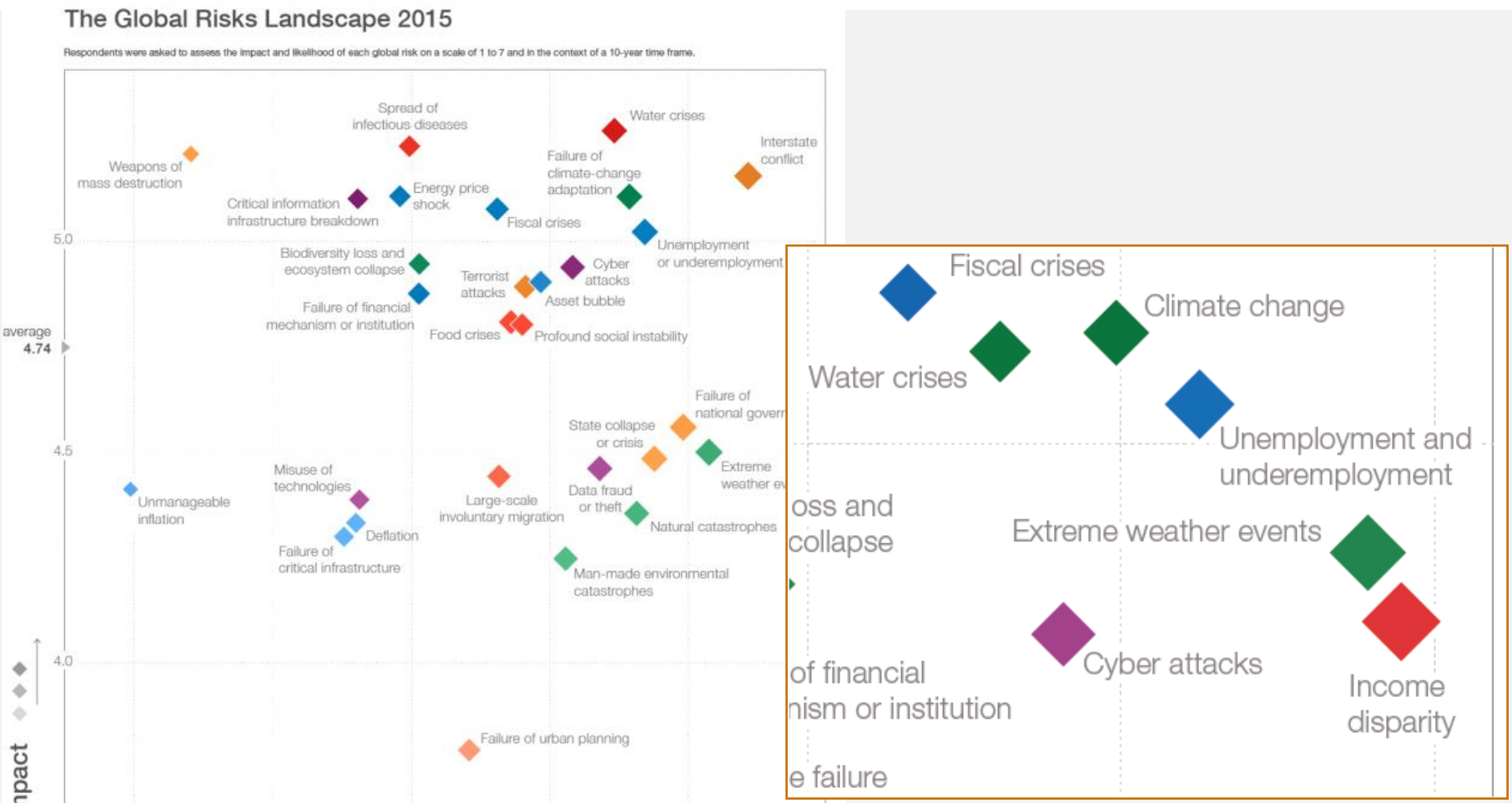
1. Cyber Risk Awareness
2. Development of Cyber Risks
3. Examples of Cyber losses
4. Marine Cyber Attacks
5. Maritime Cyber loss exposure
6. Insurance Approach
7. Summary & Outlook

Cyberrisks Awareness
„The risks of a new invention are usually ignored until a catastrophy occurs“

Munich RE

Invention	Euphoria	Catastrophy	Reaction
First Atomic Powerplant 1954	„pure, safe, cheap, efficient and clean energy“ Solution for the worlds energy problems	Chernobyl, Fukushima	Nuclear Power Phase-Out 2022 in Germany
Asbestos Manufactoring Company 1871	„one of the most versatile materials in the world“	Discovery of carcinogenic substance	Banned in most of the world
Netscape Navigator 1994	„the internet will liberate the world“	„Cyber Fukushima“ ???	???

The Global Risks 2015 Report



Source: Global Risks 2015 report, World Economic Forum, Switzerland, 2015.

Cyber Awareness in the European Union
- Maritime Sector -

Munich RE

"It was clearly noted that **the awareness regarding cyber security aspects is either at a very low level or even non-existent in the maritime sector**, this observation being applicable at all layers, including government bodies, port authorities and maritime companies."

enisa
European Network and Information Security Agency

Maritime sector is a critical infra-structure for world economy

90% of EU external trade via maritime transport

Maritime activity increasingly relies on IT

Cyber Awareness in the Middle East

Munich RE

MIDDLE EAST INSURANCE REVIEW INCORPORATING GLOBAL TAKAFUL

68%	▪ of organizations lack internal capabilities to protect against cyber attacks
62%	▪ Fail to to treat corporate data as confidential
41%	▪ Do not consider security software as necessary
45%	▪ Would drive IT security decisions only upon legislative request

Cybercrime statistics

Munich RE

Annual costs for cybercrime in comparison

Crime	Annual Costs
Drug Trafficking	$600bn
Shop Lifting	$112bn
Cybercrime	$445bn
Car Accidents	$518bn

Rank in most expensive crimes	Increase in four years	Increase in time to resolve problems	Number of hacked US companies	Estimated number of unreported cases
5	78%	130%	3.000	85%

Reliability of Cybercrime Data

Munich RE

Reliability of cybercrime data

General tendency to keep incidents secret – reputational risk!

Avoid impression to be an easy target

Avoid been seen as unsafe to customers

Unawareness of the cyber attack

Damage cannot be traced back to a cyber attack

Risk of insurance cover if physical damage is traced back to attack

Most Cyber information comes from Symantec and Kaspersky Lab

… The Present
Latest Computer Attacks – any two days in 2015 …

Munich RE

Date	Target	Description	Attack	Target Category	Attack category	Country
Feb 12	Big Fish Games	Casual gaming company Big Fish Games has its site and personal and financial information of some of its users compromised in an attack that started on last Christmas Eve.	Malware	Industry: Video Games	CC	US
Feb 14	Bter.com	China-based Bitcoin exchange Bter is hacked on Valentine‘s Day and **$1.75 million** worth of Bitcoin (7,170 BTC) is stolen.	Unknown	Bitcoin Exchange	CC	CN
Feb 14	Al Ittihad	Anonymous hackers supporting the ISIS deface Al Ittihad,UAE‘s oldest Arabic language newspaper.	Defacement	News	H	UAE
Feb 14	Nissan	An unknown Mexican hacker hacks the local Nissan account (@Nissan.mx) to find his Valentine.	Account Hijacking	Industry: Automotive	CC	MX
Feb 14	Haskell	Haskell, an advanced purely functional programming lang-uage, confirms a security breach	Unknown	Org: Non-Profit	CC	N/A

- **315.000 new viruses and malicious files detected daily**
- **500m cyber victims per year**
- **Majority of Email traffic is junk mail**

Development of Cyber Risk from a Joke to War

Munich RE

Jokes	▪ Elk Cloner
Financial & Personal Data	▪ Target, 2014, $1bn ▪ eBay, 2014, $145m ▪ MtGox, Bitcoin, 2014, 750.000 customers Bitcoins worth $446m and $500m company bitcoins stolen
Property Damage	▪ Baku-Tiflis-Ceyhan Pipeline, Turkey 2008 ▪ Stuxnet, Iran, 2010 ▪ Steel Mill, Germany, 2014 ▪ Et. Al??
Hacktivism, Terrorism	▪ Anonymous, from 2003 ▪ Estonia, 3 weeks in 2007, Russian attack
Cyber War?	▪ Sony Entertainment Pictures, 2014 ▪ Ukraine ▪ US Cyber Doctrine, 2011

Hacktivism, Terrorism
„computer crime to further religious social or political ends“

Anonymeous decentralised online community, since 2003

„100 most influencial people in the world“

Scientology, government agencies (US, Israel, Tunisia, Uganda), Visa, PayPal, Copyright Protection Agencies, KKK, Terrorists

In 2007 Estonia offended Russians after removing a soviet war memorial

Estonian government websites and commerce were disrupted

One of the largest DDoS attacks in history, paralyzing Estonia

Hacking of TV5Monde IT Infrastructure, Homepage, Facebook Account and TV Programm

After MTV biggest TV broadcastimg company worldwide

Recent Loss Examples “non-physical damage”

Munich RE

US Target Corporation, January 2014

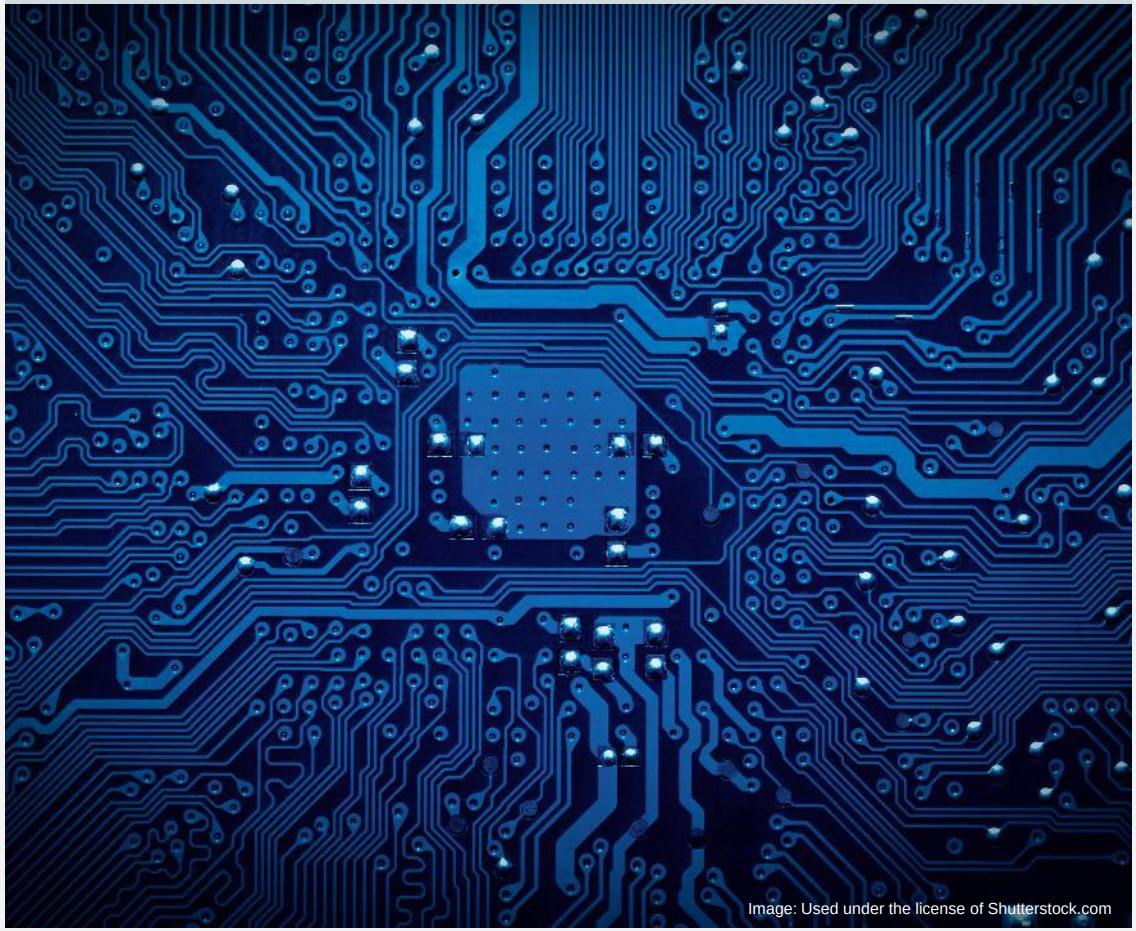
Image: Used under the license of Shutterstock.com

- A data breach of an estimated 70m credit and debit card holders took place during the the Christmas buying season.
- Indications are that the breach originated in Russia and was implemented when a contractor inadvertently opened an email that triggered the malware.
- The loss could exceed $1bn.

Recent Loss Examples “non-physical damage”

Munich RE

Sony Pictures Entertainment (SPE), 2014



- Unknown hacker group copied 100 Terabyte data from SPE servers and distributed 150 Gigabyte in the internet.
- Private phone numbers and Email accounts of all major Hollywood actors, social security numbers, credit card details, unpublished movies, salaries of all 34.000 employees and complete internal Email traffic
- Retrospective analysis showed existence of only one outer line of defense
- Hostile reactions from USA believing North Korea responsible for the hack.

Recent Loss Examples “non-physical damage”

Munich RE

One Billion bank fraud by “Carbanak”, 2014

- Hacker gang “Carbanak” steals USD1bn from 100 banks in 30 countries in the past two years.
- Email-Virus sent to bank employees tracking all computer activities, following behavior imitation.
- Manipulation of ATM’s

Recent Loss Examples “physical damage”

Munich RE

Stuxnet Virus, first discovered 2010

1. Computer worm discovered 2010, designed to attack industrial control systems

2. Worldwide infection, 58% computer infection in Iran

1. Dormiant unless Stuxnet meets specific requirements

2. Destroyed 1/5 of the Iranian centrifuges in the Atomic Plant Natanz

3. Complexity and estimated programming costs indicate national involvement

Recent Marine Loss Examples “physical damage”

Munich RE

Antwerp‘s Port Community, 2013

Reality

1. Successfull Cyber attack on the Container Logistics System of Antwerps container terminal between 2011 and 2013
2. Drug trafficers hired hackers to manipulate the logistic system
3. Containers were handed out to fake drivers
4. Discovery of 2 tons of heroine, and millions of cash

Threat

1. 420m containers shipped annually, 95% of the world trade

Recent Marine Loss Examples “physical damage”

Munich RE

AIS vessel tracking system, 2013

Reality

1. Automatic Identification System installed on 400.000 ships
2. Modification of all ship details such as position, course, flagged country, speed, name, AToN‘s (Aid to Navigation) entries, such as buoys and lighthouses.

Threat

1. Causing ship collisions, harbour blockage
2. Create fake vessels
3. Disable AIS and hide the vessel
4. Devices cost approx. $2.000

Recent Marine Loss Examples “physical damage”

Munich RE

GPS spoofing, 2013

1. In a 2013 demonstration a team of university students broadcasted false GPS signals, causing the Yacht White Rose to go on wrong course

2. Overlay of the real GPS signals with faked GPS signals

3. In contrary to GPS jamming, the spoofing is not easily detectable

4. Costs of a spoofing device: up to 3.000$

Recent Loss Examples

Munich RE

Shamoon & Night Dragon, 2012

1. 15th August 2012 Saudi Aramco had to disconnect their IT system from the Internet.

2. As a result of the Computer Virus 30.000 workstations had to be disconnected for 2 weeks.

3. Weeks later Quatari Liquid & Natural Gas had to bring their entire network down.

Marine Cyber Loss Exposure

- **Higher Probability**
- Several incidents
- High number of entry points
- Easy to target
- High exposure

- **Medium Probability**
- One reported incident
- Very limited entry points
- Difficult to target
- Medium exposure

- **Lower Probability**
- Few incidents reported
- Few entry points
- Difficult to target
- Medium exposure

Images: Used under the license of Shutterstock.com

Current Insurance Approach

Munich RE

- In general Cyber Exclusion CL380 recommended for all Marine Risks
- Wide usage of the CL380 worldwide
- Helps to protect against unexpected exposure
- only malicious attacks are excluded
- Comprehensive and well worded, but 2003 version will be updated soon
- Gap cover possible for single risks, subject to individual third party expert risk assessment.

INSTITUTE CYBER ATTACK EXCLUSION CLAUSE (CL 380) 10/11/2003

1.1 Subject only to Clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly 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 program, malicious code, computer virus or process or any electronic system.

1.2 …

Summary

Munich RE

- Cyber Risks are underestimated, awarness is low
- Cyber Risks are a business and not an IT problem
- Higher exposure and frequency in non-Marine LoB
- High loss potential in Marine
- Few examples of property damage so far but a question of time
- General exclusion of cyber risks indispensable
- Single risk acceptance possible – tailor made solutions

„SCHADENSPIEGEL“
www.munichre.com

Munich RE

TOPICS
SCHADENSPIEGEL

The magazine for claims managers
Issue 2/2014

Danger from the internet

Cyber risks are increasing and threaten many companies with losses that are both diverse and difficult to assess. PAGE 6

Third-party liability
Brain injuries in the NFL

Hail losses
Is there a risk of change?

Power plant construction
High quality standards prevent losses

TOPICS
SCHADENSPIEGEL

The magazine for claims managers

MOL Comfort

The sinking of the MOL Comfort in the Arabian Sea in mid-2013 was the costliest loss ever involving a container freighter. Growing vessel sizes and rising costs for the salvage and removal of wrecks present new challenges for the insurance industry.

© 2015 Münchener Rückversicherungs-Gesellschaft © 2009 Munich Reinsurance Company

Image: Munich Re Oliver Soulas

Thank you very much for your attention!

Alexander Kababgi, Claims Manager

Munich RE