

Maritime Cyber Insurance

Assess - Plan - Secure - Insure

Maritime Cyber Insurance

Cromar Coverholder at Lloyds



Coverholder at LLOYD'S



Contents

- Cromar Coverholder at Lloyd's
- Lloyd's Best Coverholder Innovation Award
- Maritime Cyber Risk
- AXIS Capital
- AXIS Marine Cyber Connect
- Education Engine around Maritime Cyber Risks & Cyber Insurance
- More Information

Cromar Coverholder at Lloyd's

- Cromar is a provider of corporate and specialist insurance solutions for clients within the Lloyd's markets.
- Our aim is to help our clients manage their risks and, if disaster strikes, to help them minimise disruption to their business.
- We believe in long-term relationships. So we keep in step with our clients at every stage; using our expertise to ensure our client risks stay covered in the most effective way. And if a crisis occurs, our Claims team will be at your side until our clients are back up and running.
- So our customers can look after their business, while we look after the risks.
- Lloyds Market Coverholder Innovation Award 2016 for our education engine

LLOYD'S Best Coverholder Innovation Award 2016

Winner: Cromar for their education engine around cyber risks

www.CyberInsuranceQuote.gr is the first marketplace platform of its kind dedicated exclusively to cyber insurance and an education tool around cyber and data privacy risks for small companies in Greece



[Lloyd's Market Innovation Awards](#) are a celebration of the unrivalled talent and expertise that exists in the Lloyd's Insurance Market, showcasing the excellent work the market is doing every day to innovate in an ever-changing global risk landscape.

Trends

- Cyber security **threats are progressing** and becoming a part of our daily business
- **Regulations are evolving:**
IMO-MSC 1/CIRC 1526 June 1st 2016 →
... Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping...
- The **cyber security exclusion clause** in insurance (Clause 380) is being **challenged**:
 - Owners expect complete insurance coverage
 - Underwriters need to properly manage their risks



Reported incidents around the world is increasing

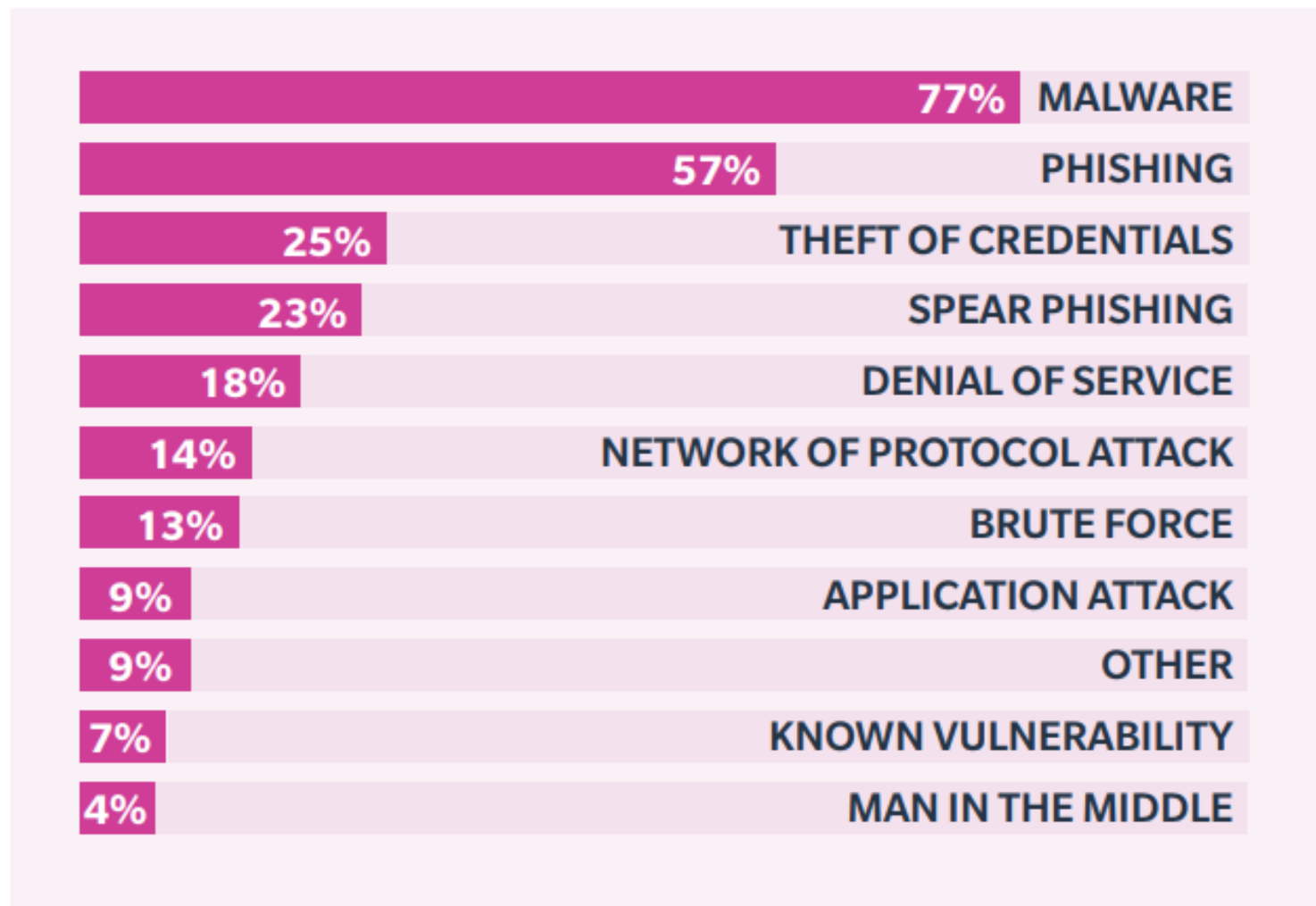


Source: DNV - GL

Cyber risks are increasing rapidly

- The annual damage to the global economy from cybercrime is estimated to be between 200–400 billion USD
- According to the CSO Alliance, more than 1,000 ships have successfully been hacked in the last five years
- After the NotPetya incident in 2017, Maersk had to reinstall its entire infrastructure including 45,000 PCs, 2,500 applications, and 4,000 servers
- **The positive message is:** Cyber security is now getting the attention within the maritime industry it deserves –but there is **not enough action yet!**

The Nature of Cyber Attacks on the Maritime Industry



Source: BIMCO and IHS Markit

Cyber Incident: NotPetya Cyber Attack

Corporate Earnings Show Impacts of NotPetya Cyber Attack

August 2, 2017 by Reuters



Transport & Logistics reiterates the expectation of an underlying profit above USD 1bn, despite expected negative result impact from the June cyber-attack estimated at a level of USD 200-300m, of which the majority relates to lost revenue in July. The vast majority of the impact of the cyber-attack was in Maersk Line.

Interim Report
Q2 2017

Source: DNV - GL

Jim Hagemann Snabe - Maersk CEO

- *"Very significant & important Wakeup call"*
- *"We were basically average when it comes to Cyber Security (like many companies)"*
- *"This was the wakeup call to become, not just good, (but also) to (arrive) in a situation where cyber security becomes a competitive advantage"*



Source: DNV – GL Video <https://youtu.be/VaqIYImDbA>

NotPetya: Heavily impacting maritime industry players

- Arrived via an update to an accounting system in Ukraine (ME Doc)
- Spread like a worm from an infected machine
- Exploited Windows SMB vulnerability (aka EternalBlue), fix by Microsoft was released on March 14th ([MS17-010](#))
- Spreads into the local network using exploits like Eternal Blue and tools like PsExec and WMIC
- Encrypts MFT (Master File Tree) tables for NTFS partitions
- Overwrites the MBR (Master Boot Record) with a custom bootloader
- Shows a ransom note demanding USD 300, same bitcoin wallet
- Prevents victims from booting their computer



"Big hack at Maersk puts Rotterdam's container terminal flat"

David Bremmer and Leon van Heel, AD, NL

Source: DNV - GL

Saudi Aramco case



The hackers were never identified or caught (that we know of)



On the morning of Wednesday, Aug. 15, 2012, files began to disappear, computers started shutting down. No more Internet, corporate email or office phones. Lengthy, lucrative deals needing signatures **had to be faxed one page at a time...**

Temporarily stopped selling oil to domestic gas tank trucks and **after 17 days Saudi Aramco relented and started giving oil away for free to keep it flowing within Saudi Arabia...**

Representatives flew directly to computer factory floors in Southeast Asia to **purchase every computer hard drive being manufactured (50,000 hard drives)...**

Everyone who bought a computer or hard drive from September 2012 to January 2013 had to pay a slightly higher price for their hard drive...

Supply specifically designed Trojan Toolkit



Mid-2012, One of the computer technicians on Saudi Aramco's information technology team opened a scam email and clicked on a bad link. The hackers were in

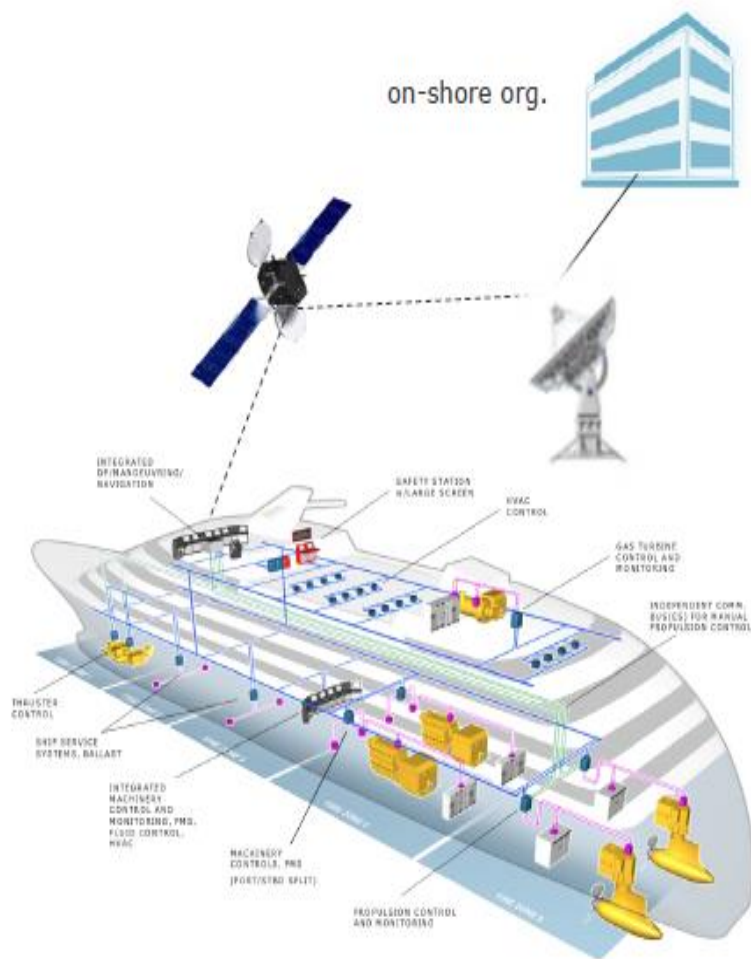


Who's interested in a Saudi Aramco breach (9.5 million barrels per day production...)?



Social engineering: Gaining understanding of emotional triggers

Safety in shipping today heavily depends on cyber systems



Information Technology (IT)

- IT networks
- E-mail
- Administration, accounts, crew lists, ...
- Planned Maintenance
- Spares management and requisitioning
- Electronic manuals
- Electronic certificates
- Permits to work
- Charter party, notice of readiness, bill of lading...

At risk:

Mainly
finance
and
reputation

Operation Technology (OT)

- On-board measurement and control
- ECDIS
- Power management
- GPS, CCTV
- Remote support for engines
- Data loggers
- Engine control
- Dynamic positioning, ...
- PLCs

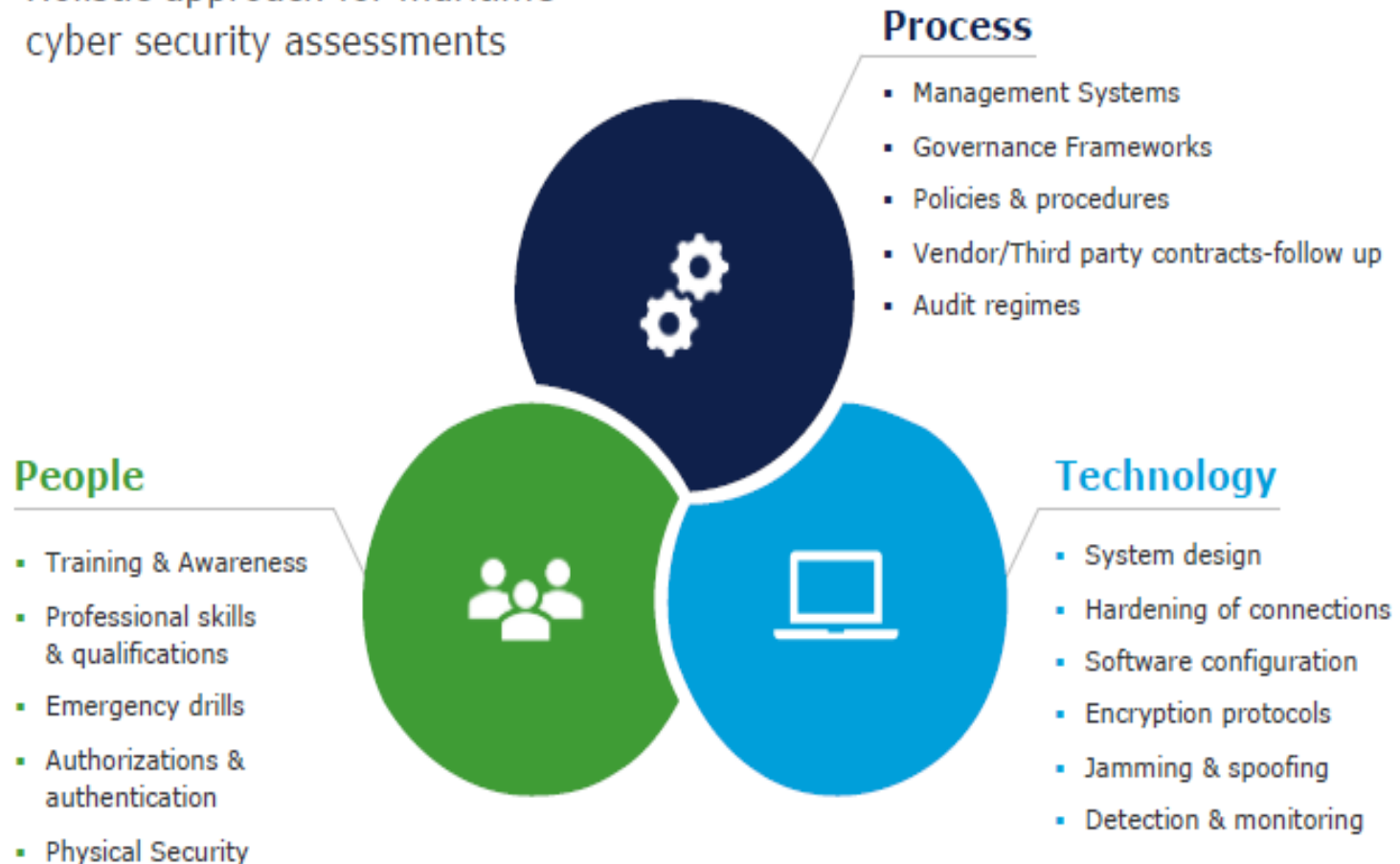
At risk:

Life,
property
and
environment
+
all of the
above

Source: DNV-GL

Three Pillars of Cyber Security

- Holistic approach for maritime cyber security assessments



Source: DNV-GL

Residual Risk – Risk Transfer to Cyber Insurance Carrier



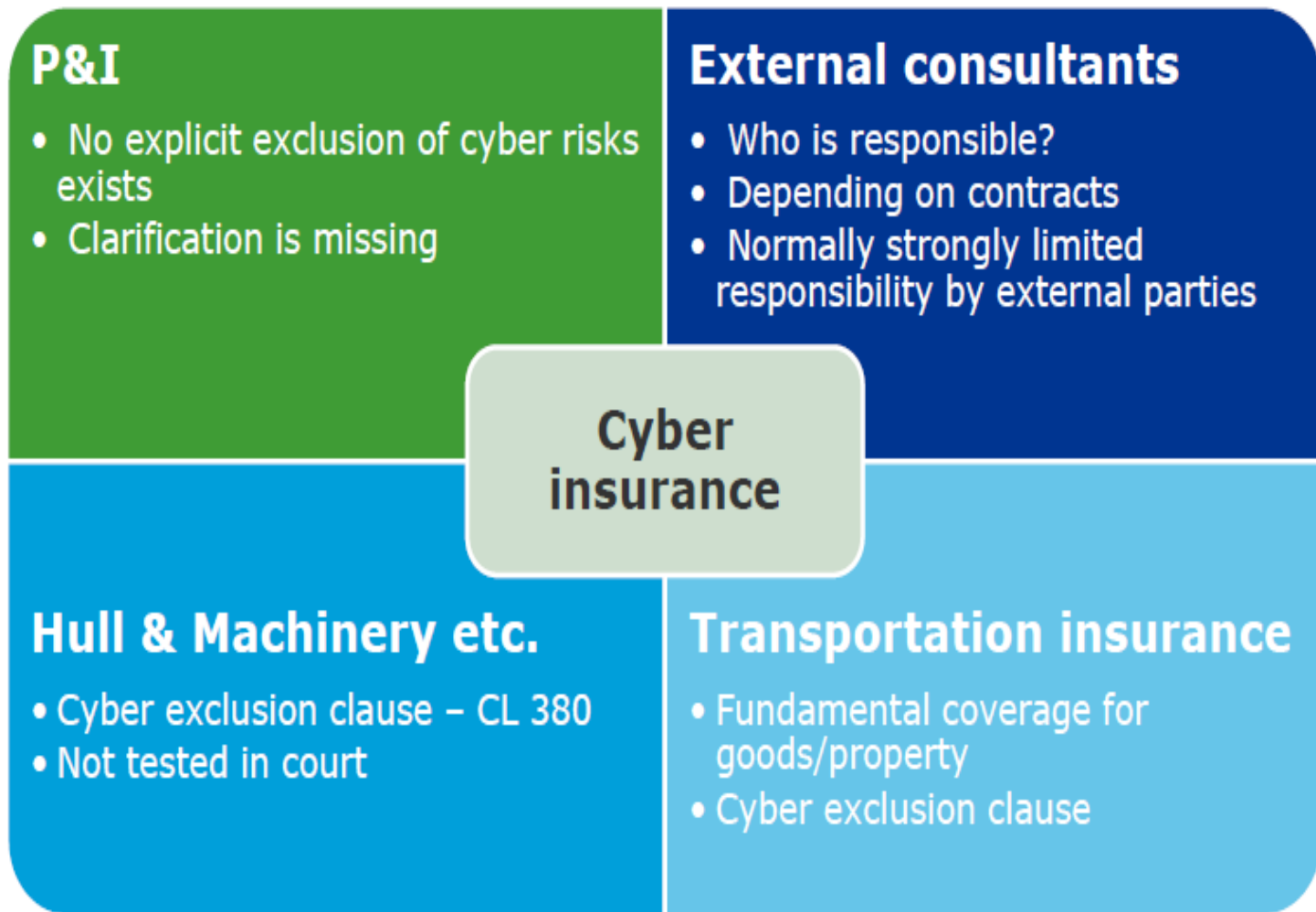
Maritime Cyber Risks

- **ONSHORE** risk is similar to the cyber threat facing any business. The primary concerns include the loss of income from business interruption, as well as the logistics of, and the expense incurred in, restoring affected systems and paying any extortion demands.
- **OFFSHORE** risk is any risk occurring on board the vessel that leads to a physical damage loss, from pilots using an infected USB stick which takes the system down leading to the vessel grounding, to the vessel system being maliciously attacked by a third party resulting in a collision. Of course, any cyber threat that could lead to physical damage to the vessel could also lead to costly business interruption and system restoration cost as well.

Maritime Cyber Risks - CL380 Cyber Exclusion Clause

- Over recent years, the marine insurance market has mainly been concerned with the offshore risk, and hence the **CL380 Cyber Exclusion Clause** has been added to Hull and Machinery Insurance policies in order to exclude the risk of physical damage caused by a malicious cyber attack. However, as paper charts have given way to technical onboard systems, thereby increasing the cyber risk, concerns have grown over the gap in insurance coverage created by the CL380 Exclusion.
- Equally, the cost of business interruption caused by a cyber attack is being increasingly felt in the maritime industry, and with tight business margins, owners want the reassurance of being insured.

Cyber Insurance as a Risk Management Tool



Axis Marine Cyber Connect

- Incident Management & Response 24/7/365
- First Party Insuring Agreements
- Third Party Insuring Agreements

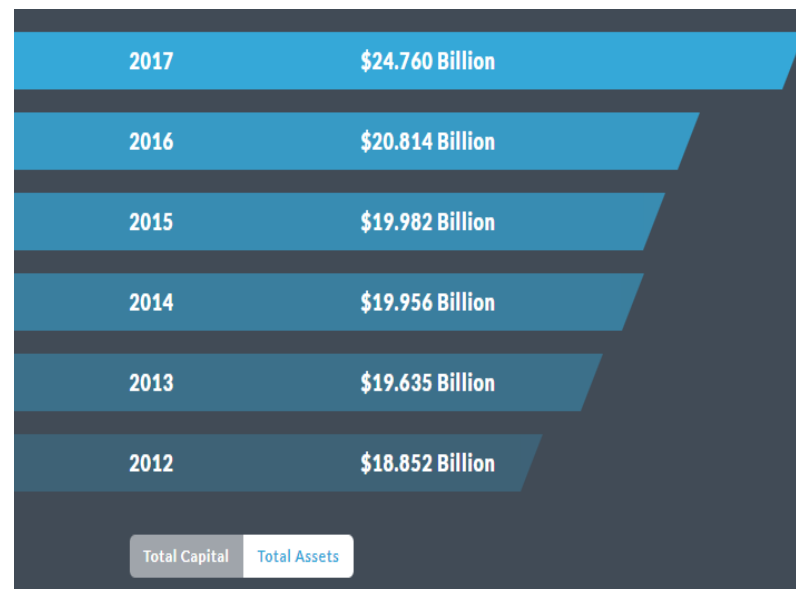


LLOYD'S

THE WORLD'S SPECIALIST
INSURANCE MARKET

Axis Capital

- We offer specialty insurance and reinsurance through AXIS' managed Syndicates 1686 and 2007 at Lloyd's.
- As a Lloyd's Corporate Member, AXIS Corporate Capital UK Limited provides capital for the Syndicate.
- We underwrite property, casualty, professional lines, marine, energy, aviation, terrorism, surety, cyber, environmental, political risk, credit risk and others.



Axis Marine Cyber Connect

AXIS Marine Cyber covers:	AXIS Marine Cyber	Standard Hull Insurance	Standard Cyber Insurance
Breach Response Costs and System Restoration	✓	X	✓
Physical Damage to the Vessel	✓	Infrequently	X
Income Loss & Expenses from a Breach	✓	X	✓
Third Party Costs and Regulatory Fines	✓	X	✓
Access to Pre-Breach Education	✓	X	Occasionally
Access to Specialists During a Breach	✓	X	✓

First Party Insuring Agreements

A. Maritime Cyber Response Costs

Underwriters will pay on behalf of the Insured for any Breach Response Costs arising out of an actual or suspected Network Security Breach, Privacy Breach or a Confidentiality Breach that first occurs on or after the Retroactive Date and is Discovered during the Policy Period.

Breach Response Services Offered

- Breach coaching
- PR
- IT Forensics

Example

A member of IT authorises a software update and computers around the office and on board vessels immediately shutdown. The insured suddenly find they are unable to access their system, because it has been corrupted with malicious software. Who would they call for help? Our Breach Response helps to guide the insured through any situation, meaning the business can be back up and running as smoothly and as quickly as possible, with minimal business interruption.

How it works

If the insured suspects they have had a Network Security/Privacy/Confidentiality Breach that is discovered during the policy period, they will be able to appoint a company from the list of Pre-Approved Providers from the Axis Maritime Cyber Response Panel.

They can incur Breach Response Costs without first obtaining Underwriters prior consent for the period of time listed in the conditions.

First Party Insuring Agreements

B. Maritime IT System Restoration Costs

Underwriters will pay the Insured for any Restoration Costs incurred as a direct result of damage to the Insured's Data or Insured's Programs caused by:

- Computer Attack;
- Any Operational Error;
- Accidental damage of hardware;
- Failure of back-up generators; or
- Electrostatic build-up and static electricity;

Example

One of the crew has used their USB stick onboard a vessel. It is infected with Malware which attacks all vessel networks, causing loss of bridge systems and the inability to operate the ship. All computers are down meaning that systems including charter parties, access to contacts, logistic control, ECDIS/AIS systems cannot be used. We will pay for the system to be restored to get the business up and running as quickly as possible.

How it works

If the insured has any damage to their data or programs caused by anything listed, we will pay for the restoration.

First Party Insuring Agreements

C. Insured's Network Failure - Income Loss and Extra Expense

Underwriters will pay the Insured for any Income Loss and Extra Expense incurred by the Insured due to the suspension or deterioration of the Insured's business during the Period of Restoration, provided that the duration of such interruption, degradation or failure was directly caused by:

- Computer Attack;
- Any Operational Error;
- Accidental damage of hardware;
- Failure of back-up generators; or
- Electrostatic build-up and static electricity;

Example Onshore

The insured receive numerous calls from customers who cannot access the booking system on their website or trace their cargo. They discover they are under a Distributed Denial of Service Attack. Whilst the system is being restored, they cannot receive any bookings, operate any of their vessels or contact any of their clients. We will pay for the loss of income and extra expense during this period of inactivity or reduced efficiency.

Example Onboard

The Master has received an attachment from the 'port authority' with allotted times for berthing operations. The email was fake and the attachment was malicious and as a result has considerably slowed down the onboard IT systems. This has led to the Master not being able to berth on time, leading to ongoing delays for a week whilst they wait for the systems to be restored (paid for under section B). We will cover the insureds loss of income and extra expense during this period of inactivity or reduced efficiency.

How it works

If the insured experience Income Loss and Extra Expense due to suspension or deterioration of their business during the Period of Restoration, it is covered provided it was caused by any of the items listed.

This is similar to the traditional LOH cover found in Marine Hull policies

First Party Insuring Agreements

D. Outsource Service Provider - Income Loss and Extra Expense

Underwriters will pay the Insured for any Income Loss and Extra Expense incurred by the Insured due to the suspension or deterioration of the Insured's Business during the Period of Restoration directly as a result of the total or partial interruption, degradation in service or failure of a Network operated by an Outsource Service Provider for the Insured, provided that the duration of such interruption, degradation or failure was directly caused by:

- Computer Attack;
- Operational Error;
- Accidental damage of hardware;
- Failure of back-up generators; or
- Electrostatic build-up and static electricity

Example

The insureds IT service provider has been hit with a ransomware attack that has left them unable to service their company. As a result, the shipping operations have stalled because they cannot locate cargo manifests, take bookings etc.

How it works

We will pay if the insured experiences Income Loss and Extra Expense due to suspension or deterioration to business during the Period of Restoration because systems operated by an Outsource Service Provider fail or are interrupted by one of the items listed.

The cover here is as per coverage C but for events that take down IT vendors that the insured relies on as opposed to an attack on the insured's network itself.

First Party Insuring Agreements

E. Cyber Extortion and Ransomware

Underwriters will reimburse the Insured for any Cyber Extortion/Ransomware Payments and any Cyber Extortion/Ransomware Expenses incurred directly as a result of a Cyber Extortion Demand or Ransomware Demand first made against the Insured during the Policy Period and reported to the Underwriters.

Example

The crew on board a vessel connects to the Wi-Fi at a port which is infected with ransomware. The computer network shuts down because the data has been encrypted and a ransom notice appears demanding payment for access to the network. If the system cannot be restored from back-ups with assistance from the Breach Response Team, we will reimburse the extortion payment and expenses incurred.

How it works

If the insured experiences any Cyber Extortion or Ransomware Demand we will reimburse any payments and expenses incurred.

Third Party Insuring Agreements

F. Third Party Insuring Agreements

The Policy provides the Insured with coverage for Claims made under the following Insuring Agreements;

1. Network Security, Privacy and Confidentiality Liability

Underwriters will pay on behalf of the Insured any Damages and Defense Costs arising out of a Claim first made against the Insured during the Policy Period alleging a Network Security Breach, Privacy Breach or a Confidentiality Breach that first occurs on or after the Retroactive Date and prior to the end of the Policy Period.

Example

An employee inadvertently sends malware to a third party/client causing them to experience Network Damage and Business Interruption loss. We will pay for damage and defense costs arising from this claim.

How it works

If a claim is made against the insured alleging a Network Security, Privacy or Confidentiality Breach we pay any damages and defence costs arising from this claim. We will also pay any Regulatory Penalties/Investigation Costs arising out of a Regulatory Claim. Our Breach Response Services will be able to advise the insured on their obligations and the types of fines/penalties that could be imposed.

Third Party Insuring Agreements

F. Third Party Insuring Agreements

The Policy provides the Insured with coverage for Claims made under the following Insuring Agreements;

2. Network Security and Privacy Liability (Regulatory)

Underwriters will pay on behalf of the Insured any Regulatory Penalties and Regulatory Investigation Costs arising out of a Regulatory Claim first made against the Insured during the Policy Period alleging a Network Security Breach, Privacy Breach or a Confidentiality Breach that first occurs on or after the Retroactive Date and prior to the end of the Policy Period.

Example

The insured experiences a loss of customer/client information resulting in a claim being brought against the insured claiming damages. We will pay for damage and defense costs arising from this claim.

How it works

If a claim is made against the insured alleging a Network Security, Privacy or Confidentiality Breach we pay any damages and defence costs arising from this claim.

We will also pay any Regulatory Penalties/Investigation Costs arising out of a Regulatory Claim. Our Breach Response Services will be able to advise the insured on their obligations and the types of fines/penalties that could be imposed.

Third Party Insuring Agreements

G. Cyber Attack CL380 Buyback

Underwriters will pay the Insured for any losses expressly excluded by the marine Insurers under the Designated Maritime Policy listed on the Policy Schedule due to the Institute Cyber Attack Exclusion Clause (CL 380 November 2003 edition)

Example

A GPS jamming criminal syndicate are testing out their GPS jamming signals off the coast of Dover, one of the World's busiest shipping routes. Attacks on GPS are followed by threats that the vessel is in a dangerous position unable to find her precise location to continue the trip or manoeuvre back to port. Because the unavailability of data and the connectivity with the AIS, the ECDIS and VDR devices on board when GPS is 'jammed' all of the above devices are affected. As a consequence, the vessel collides into another vessel which is laid up at anchor causing significant damage to both vessels.

Example

A pilot gets on board a vessel with an infected USB stick. This infects the on board system with malware and over the course of a few hours takes the system down, making it unusable. The vessel has no access to GPS/AIS/ECDIS and whilst attempting to get back to port, grounds on a sandbank creating significant damage to the Hull.

How it works

We will pay for any losses that would otherwise be covered but are excluded due to the CL380 cyber exclusion clause.

Third Party Insuring Agreements

H.Customer Cargo Damage Mitigation Clause

Where there has been a Network Security Breach that results in the potential for damage and/or deterioration to customer cargo and this may result in a Claim under Section F1 above (Network Security, Privacy and Confidentiality Liability), Underwriters will reimburse the Insured for Mitigation Costs, incurred by the Insured and consented to by the Underwriters at the Underwriters' sole discretion.

Example

The insured experiences a network failure which means they have no access to their computers. They therefore have no access to the bills of lading, causing severe delays to the delivery of the customer's cargo. We will cover the costs of re-warehousing and the additional logistical costs of relocating this cargo until it can be redelivered to the client.

Notice

The covers descriptions are for preliminary informational purposes only. The exact coverage afforded by the product(s) described are subject to and governed by the terms and conditions of each policy issued.

How it works

We will cover the costs associated with mitigating a liability claim arising from a Network Security, Privacy and Confidentiality Liability event which have the potential to damage and/or deteriorate customer's cargo.

Education Engine around Maritime Cyber Risks & Insurance

www.maritimecyberinsurance.com



[HOME](#) [CYBER RISKS](#) [CYBER INSURANCE](#) [GDPR](#) [ACADEMY](#) [BLOG](#) [CONTACT](#)

Maritime Cyber Insurance

Assess - Plan - Secure - Insure

Maritime Cyber Risk

Education Engine around Maritime Cyber Risks & Insurance

www.maritimecyberinsurance.com



[HOME](#) [CYBER RISKS](#) [CYBER INSURANCE](#) [GDPR](#) [ACADEMY](#) [BLOG](#) [CONTACT](#)

CYBER RISK
AWARENESS

CYBER RISKS &
SHIPPING

CYBER SCAMS

RANSOMWARE

CYBER SECURITY

IMO

INCIDENTS

Maritime Cyber Insurance

Assess - Plan - Secure

Maritime Cyber Risk



Maritime Cyber Insurance

Assess - Plan - Secure - Insure

Maritime Cyber Insurance

Nikos Georgopoulos

Cyber Privacy Risks Advisor

Email: nikos.georgopoulos@cromar.gr

Cromar Coverholder at Lloyd's

17.Ag Konstantinou & Ag Anargiron St

151 24, Attica Maro;usi

www.cromar.gr

www.maritimecyberinsurance.com

email: info@cromar.gr



Coverholder at LLOYD'S