STEAMSHIP CYBER COVER

The IMO has adopted a resolution which requires companies, no later than the first annual verification of their Document of Compliance (DOC) after 1 January 2021, to demonstrate that cyber security is an integral part of their safety management system. The maritime world is seeing a sharp increase in cyber-attacks and so cyber security and safety is important to protect a shipowner's operations. BIMCO have introduced a Cyber Security contract clause which sets out the responsibilities of each party, defining what is expected from both sides both before and after a cyber event. The ability to react quickly and effectively to any breach of cyber security is vital to ensuring the cyber safety of the vessel.

Whilst there is no cyber exclusion in a Member's P&I cover in respect of liabilities which may be caused through a cyber event, Members may still be left uninsured for the costs of restoring their systems and data and for losses where a vessel is put off hire or is unable to trade as a result of a cyber-attack.

The Club's new Cyber Insurance product is aimed at assisting Members respond to a cyber-attack on their vessels and insuring them for any loss of income the vessel incurs as a result.

Scope of Cover

Cover is only in respect of events affecting an entered vessel and does not extend to shoreside offices or other property.

Limit: US$10m in the aggregate per fleet per policy year. US$1m per vessel per event.

Agreed Daily Indemnity: This will usually be equivalent to the expected charter hire and is set at the beginning of the policy.

Deductible: One deductible for sections A, B & E and 1 day's Agreed Daily Indemnity seperately for C & D.

A – **Maritime Cyber Response Costs** – costs arising out an actual or suspected network security breach.

B – **Maritime IT System Restoration Costs** – restoration costs as a result of damage to Data or programs.

C – **Income Loss and Extra Expense** – Agreed Daily Indemnity, less any income earned, where loss is incurred due to suspension or deterioration of vessel operations during the restoration of systems/data

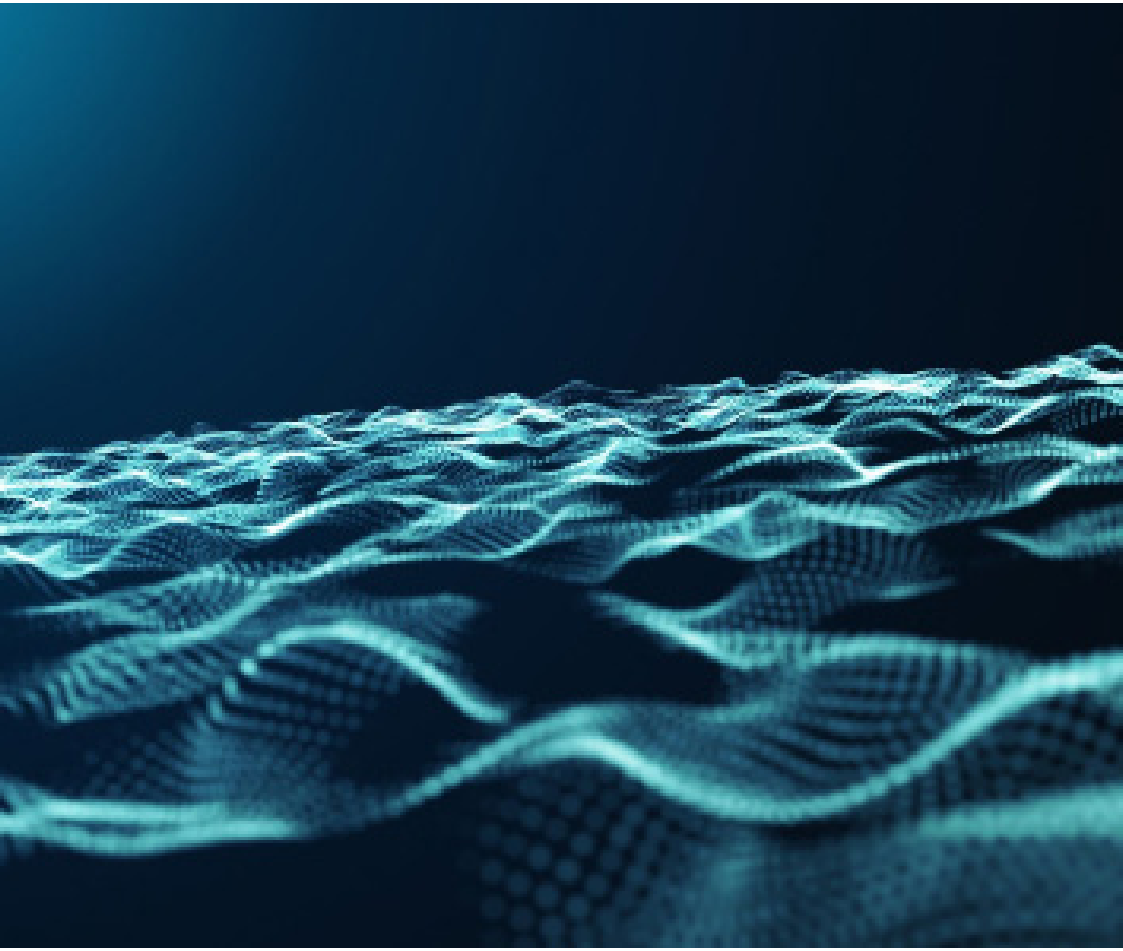
D – **Income Loss and Extra Expense – Outsource Service Provider** – Agreed Daily Indemnity, less any income earned, where loss is incurred due to suspension or deterioration of vessel operations during the restoration of systems/data belonging to an outsource provider.

E – **Cyber Extortion & Ransomware** – covers ransomware payments and expenses incurred.

Taking out this cover, not only gives Members protection for

losses arising out of a cyber-attack, but also gives Members quick access to cyber experts who can respond to the incident and assist the Members resolve any issues.

Members who purchase the cover will benefit from a free Maritime Cyber Security Awareness education course, which focuses on increasing crew awareness of cyber threats. Your crew will learn the benefits of reporting all cyber incidents. As well as 10 essential steps to maritime cyber security, the course includes modules on Cyber threat, Phishing, Surfing the web, Malware & Insider threat.



Members can also view the Club's Cyber Security film on the Club's website.

This product is available to all vessels operated by Members, including those not entered for P&I, and non-Members. Initially this product will not be available for yachts or passenger vessels.

Cover detail and Scenarios

A. Maritime Cyber Response Costs

The Club will indemnify the Member for any Cyber Incident Response Costs arising out of an actual or suspected Network Security Incident that first occurs on or after the Cover Inception Date and is discovered during the Policy Period.

Cyber Incident Response Services offered:

- Cyber incident coaching
- Crisis communication and public relations
- IT forensics

Example

A member of IT authorises a software update and computers onboard vessels immediately shutdown. The Member suddenly finds they are unable to access their system, because it has been corrupted with malicious software. Who would they call for help? Our Cyber Incident Response team is available 24/7 to help guide the Member through any situation, meaning the vessel can be back up and running as smoothly and as quickly as possible, with minimal business interruption.

How it works:

If the Member suspects they have had a Network Security cyber

incident that is discovered during the policy period, they will be able to call the 24/7 telephone number contained within their policy to get assistance and coaching throughout the event. Whilst it is always advisable to contact the Club immediately, Cyber incident costs can be incurred without first obtaining the Club's prior consent for the period of time and monetary amount listed in the policy schedule.

B. Maritime IT System Restoration Costs

The Club will indemnify the Member for any Restoration Costs incurred as a direct result of damage to the Member's Data or the Member's Programs caused by:

- Computer incident;
- 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 impacts the vessel networks. Various systems are affected, and the vessel will not be able to navigate safely until the networks have been restored. We will cover the costs incurred for the system to be restored to get the business up and running as quickly as possible.

How it works:

If the Member has any damage to their data or programs caused by anything listed above, we will indemnify the Member for the restoration costs incurred by external consultants as well as the Member's own expenses incurred in restoring, repairing, recreating or replacing damaged data or programmes to their original pre-damage condition.

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

The Club will indemnify the Member for an Agreed Daily Indemnity, which represents any Income Loss, and Extra Expense incurred by the Member due to the suspension or deterioration of the vessel's business during the Period of Restoration directly as a result of the interruption or failure of the Member's Network, provided that the duration of such interruption, degradation or failure was directly caused by:

- Computer incident;
- Any operational error;
- Accidental damage of hardware;
- Failure of back-up generators; or
- Electrostatic build-up and static electricity;

The Member's Network, includes the networks of co-assured Managers.

Example

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 which caused certain IT systems to be impacted. This has led to the Master not being able to berth on time, leading to ongoing delays for two days whilst they wait for the network to be restored (paid for under section B). We will indemnify the Member's loss of income

(Agreed Daily Indemnity) and extra expense during this period of inactivity or reduced efficiency.

How it works

If the Member experiences Income Loss and Extra Expense due to the suspension or deterioration of their business during the Period of Restoration, it is covered provided it was caused by any of the items listed above. This is similar to Loss of Hire policies.

D. Outsource Service Provider – Income Loss and Extra Expense

The Club will indemnify the Member for an Agreed Daily Indemnity, which represents any Income Loss, and Extra Expense incurred by the Member due to the suspension or deterioration of the vessel'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 Member, provided that the duration of such interruption, degradation or failure was directly caused by:

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

Example

The Member's IT service provider has been hit with a ransomware incident that has left them unable to service the vessel. As a result, the shipping operations have stalled because of their reliance on the IT service provider.

How it works:

The cover here is as per coverage C (on the previous page) but covers failure of a network operated by an Outsource Service Provider for the Member as opposed to an incident on the Member's network itself.

E. Cyber Extortion and Ransomware

The Club will indemnify the Member 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 Member during the Policy Period and reported to the Club.

Example

The crew on board a vessel connect 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 Cyber Incident Response Team, we will reimburse the extortion payment and expenses incurred.

If Members or their brokers have any questions or wish to receive a quote, please get in touch with your usual Underwriting contact.

London

Limassol

Hong Kong

Rio De Janeiro

Piraeus

Singapore

Tokyo

STEAMSHIP MUTUAL

Steamship Insurance Management Services Limited
Aquatical House
39 Bell Lane
London
E1 7LU

+44 (0)20 7247 5490 &
+44 (0)20 7895 8490
www.steamshipmutual.com
@SteamshipMutual
Steamship Insurance Management Services

Download our two apps:
Steamship Mutual and A Team Effort

Download on the App Store
GET IT ON Google Play