



Maritime Cyber Insurance Covers Fact Sheet

www.maritimecyberinsurance.com

Cyber risk policies tend to include the following policy sections either as standard wording or by specific endorsement. Specifically, the cyber risk policy covers:

Incident Management & Response 24/7/365

After the initial triage process, you will be assigned a dedicated and experienced claims handler that will act as your primary point of contact throughout the lifecycle of the claim. Your contact will be able to support you during and after an incident, including:

- Providing access to our extensive partner network, including offering advice as to the right companies to use to resolve your particular incident quickly and cost effectively
- Coordinating the incident response and carefully reviewing the scope of work and performance of the specialist teams, ensuring that the incident is handled within the scope of your policy and alerting you when this is not the case.
- Providing central communication and a single point of contact to ensure that you and your key stakeholders are kept up to date with the progress of any claim

First Party Insuring Agreements

1. Maritime Cyber Response Costs

Maritime Cyber Breach Response Costs mean:

- Reasonable and necessary costs and expenses to engage a lawyer as a breach coach** to handle, respond and project manage the breach; notify the population impacted or potentially impacted by a breach. This shall specifically include legal expenses and other costs incurred to determine whether a suspected breach is in fact a breach.
- Reasonable and necessary costs and expenses to appoint a public relations consultant** to aid the Insured in mitigating the reputational damage caused by a Network Security Breach, Privacy Breach, or a Confidentiality Breach.
- Reasonable and necessary forensics costs and expenses** incurred for the purposes of conducting a review or investigation of the source or cause of an actual or suspected Network Security Breach and to terminate the Network Security Breach.

2. Maritime IT System Restoration Costs

Restoration Costs up to the Limit of Liability incurred as a direct result of damage to the Insured's Data or Insured's Programs caused by:

- a. Computer Attack;
- b. Any Operational Error;
- c. Accidental damage of hardware;
- d. Failure of back-up generators; or
- e. Electrostatic build-up and static electricity;



Maritime Cyber Insurance Covers Fact Sheet

www.maritimecyberinsurance.com

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

The Insurer 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 the Insured's Network, provided that the duration of such interruption, degradation or failure exceeds the Time Retention and was directly caused by:

- a. Computer Attack;
- b. Any Operational Error;
- c. Accidental damage of hardware;
- d. Failure of back-up generators; or
- e. Electrostatic build-up and static electricity

4. Outsource Service Provider - Income Loss and Extra Expense

The Insurer 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 exceeds the Time Retention and was directly caused by:

- a. Computer Attack;
- b. Any Operational Error;
- c. Accidental damage of hardware;
- d. Failure of back-up generators; or
- e. Electrostatic build-up and static electricity

5. Cyber Extortion and Ransomware

The Insurer 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.

6. Cyber Crime

Crime cover for electronic wire transfer fraud

Third Party Insuring Agreements

1. Network Security, Privacy and Confidentiality Liability

The Insurer will pay on behalf of the Insured any Damages and Defense Costs, arising out of a Claim alleging a Network Security Breach, Privacy Breach or a Confidentiality Breach.

2. Network Security and Privacy Liability (Regulatory)

The Insurer will pay on behalf of the Insured any Regulatory Penalties and Regulatory Investigation Costs arising out of a Regulatory Claim alleging a Network Security Breach, Privacy Breach or a Confidentiality Breach.



Maritime Cyber Insurance Covers Fact Sheet

www.maritimecyberinsurance.com

Cyber Attack CL380 Buyback

The Insurer will pay the Insured for any losses expressly excluded by the marine Insurers under the Designated Maritime Policy due to the Institute Cyber Attack Exclusion Clause (CL 380 November 2003 edition), provided that these losses would otherwise have been covered.

Customer Cargo Damage/Deterioration 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 Insuring Agreement Network Security, Privacy and Confidentiality Liability' of the Policy, Insurer will reimburse the Insured for Mitigation Costs, incurred by the Insured

Notice

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