UK DEFENCE CLUB

Soundings

BIMCO publishes Cyber Security Clause

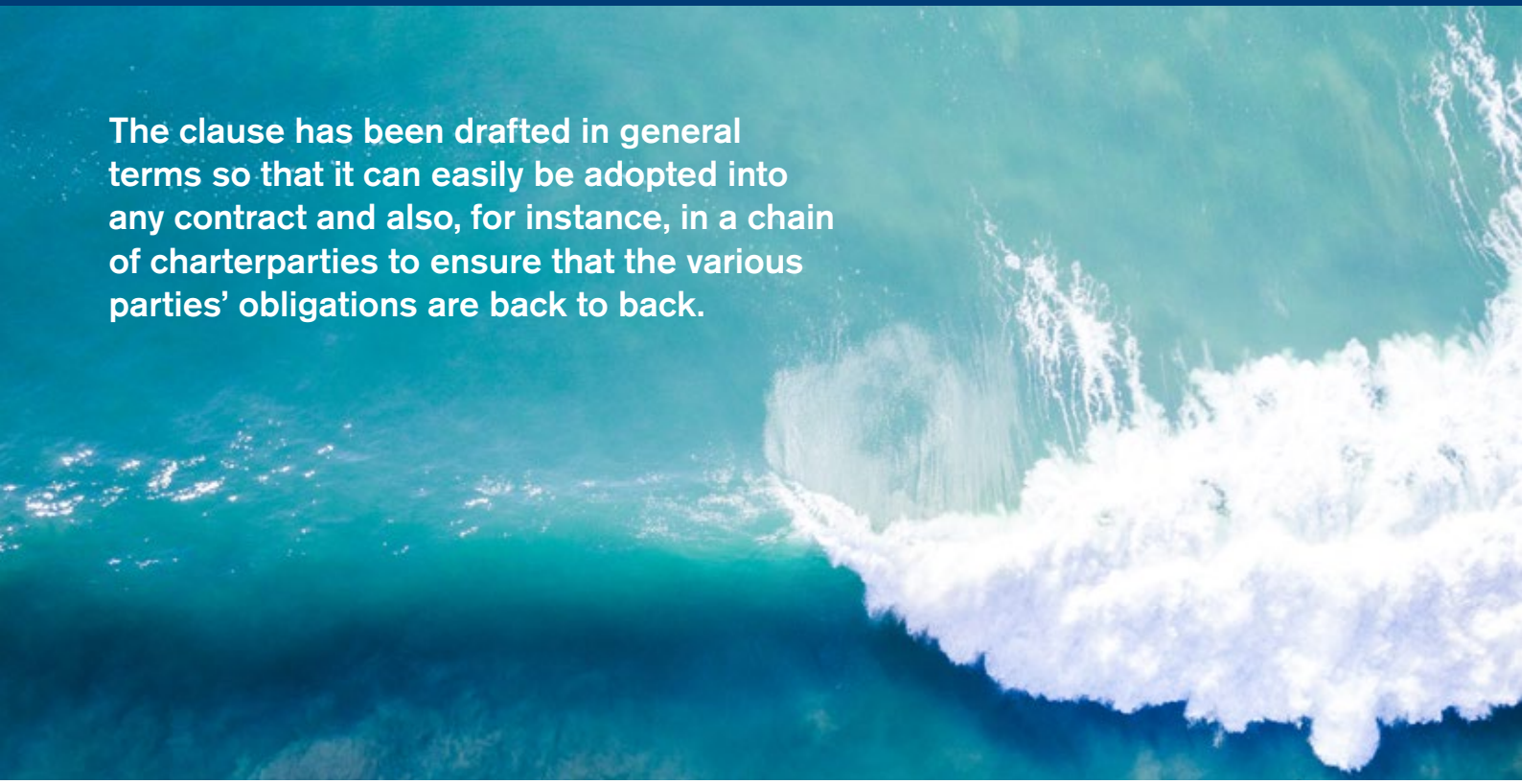
As cyber crime is becoming an ever more prevalent risk for the shipping industry, BIMCO have published a Cyber Security Clause for use in charterparties and other contracts.

Background

With the industry's increased reliance on technology comes greater exposure to cyber risk. Ships and shipping systems are potentially vulnerable to cyber attacks which are becoming ever more sophisticated and can have highly detrimental impacts. A spate of attacks on high profile shipping companies has recently brought this issue to the fore.

The IMO has given shipowners and managers until 2021 to include cyber security management procedures in their Safety Management Systems, as defined in the ISM Code. Cyber security guidance has been issued by various key bodies including the IMO, BIMCO and Intertanko, which can be provided upon request.

continued overleaf



The clause has been drafted in general terms so that it can easily be adopted into any contract and also, for instance, in a chain of charterparties to ensure that the various parties' obligations are back to back.

In this context, the BIMCO Documentary Committee has now published a standard Cyber Security Clause to provide a clear framework for apportionment of liabilities and definition of the parties' respective cyber security obligations under a contract.

The clause has been drafted in general terms so that it can easily be adopted into any contract and also, for instance, in a chain of charterparties to ensure that the various parties' obligations are back to back.

The clause

The BIMCO clause has four main constituent parts, as follows:

- In the first part, the obligations of the contractual parties are set out. These are, in line with the requirements of the ISM Code, to implement and have in place cyber security measures; to have in place measures to enable each party to respond to a cyber security incident; and, finally, to regularly review such measures / arrangements to ensure that they are up to date with current developments.

- The purpose of the second limb of the clause is effectively to impose an obligation on each party to use reasonable endeavours to ensure that any third party involved in the performance of the contract (e.g. subcontractors appointed by either party) also complies with the requirements set out in the first part of the clause.

- The third part of the clause sets out the practical steps that the parties must take in case a cyber security incident occurs. This requires prompt notification of the incident to one's counterparty and provision of follow-up information and advisory measures once there has been an opportunity to investigate the circumstances of the incident. Importantly, it is to be noted that each party has an ongoing obligation to share information which may assist the other in mitigating the effect of any cyber security incident.

- Finally, in the last paragraph of the clause the parties are free to set a limit to their liabilities for breaches of their cyber security obligations.

The importance of adopting appropriate cyber security measures in today's cyber-orientated world cannot be underestimated. The use of suitable cyber security clauses is an essential part of this and Members are therefore advised to give careful thought to such provisions when drafting new contracts.

Members are invited to contact the Managers for further information relating to the above issues.

The UK Defence Club
Thomas Miller Defence Ltd, 90 Fenchurch Street, London, EC3M 4ST
tel: +44 207 283 4646 fax: +44 207 204 2131
email: tmdefence@thomasmiller.com web: ukdefence.com