News 16 Jun, 2020

BIMCO Cyber Clause

While Covid-19 has shown the need for cyber security and good cyber hygiene, there are also regulatory reasons why the shipping community needs to put these topics at the forefront of their corporate planning.

The isolation requirements of the Covid-19 pandemic have highlighted the importance of a robust communications infrastructure and secure remote access to computer systems. It has also shown the adaptability of the cyber-criminal seeking to exploit the vulnerable and the unprepared. The world is now digitised, connected and integrated; without the ability to work remotely and securely the current economic crisis caused by the pandemic would be deeper and the mortality rate far greater.

While Covid-19 has shown the need for cyber security and good cyber hygiene, there are also regulatory reasons why the shipping community needs to put these topics at the forefront of their corporate planning. In June 2017 the International Maritime Organisation (IMO) published *Resolution MSC 428/98 Cyber Risk Management in Safety Management Systems*, which mandated that "*cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the Document of Compliance after 1 January 2021".* Most owners will consequently soon face a legal obligation to include cyber risk preparedness in their ISM procedures and documentation.

To accompany Resolution MS 428/98 the IMO has published *Guidelines on Maritime Cyber Risk Management MSC-FAL.1/Circ.3 Annex*, setting out a framework for the issues industry should take into consideration when establishing cyber risk management requirements for Safety Management System (SMS) certification. Cyber security guidance has also been published by several organisations, including BIMCO, the International Chamber of Shipping and some Classification Societies.

BIMCO clause

In June 2019 BIMCO issued a Cyber Security Clause 2019 for incorporation in a wide range of maritime contracts. The clause provides an allocation between the parties of their respective cyber security obligations under the contract and the actions each must take in the event of an incident. It is drafted in general terms to enable easy incorporation into charterparties and chains of charterparties on a back-to-back basis so that all parties to a voyage have the same cyber obligations.

In June 2019 BIMCO issued a Cyber Security Clause 2019 for incorporation in a wide range of maritime contracts. The clause provides an allocation between the parties of their respective cyber security obligations under the contract and the actions each must take in the event of an incident. It is drafted in general terms to enable easy incorporation into charterparties and chains of charterparties on a back-to-back basis so that all parties to a voyage have the same cyber obligations.

The clause is written in four main sections. The first part sets out the obligations of the contractual parties to maintain appropriate cyber security measures and to also have procedures in place to enable each party to respond to a cyber incident. There is an obligation to regularly review these arrangements to ensure that they remain fit for purpose in light of developments in technology and the risks posed.

But this sub-clause is made intentionally vague through the use of the word “appropriate” when describing the measures the parties should maintain. Whilst owners post-1 January 2021 will undoubtedly be relying upon the procedures in their SMS, there is no indication as to what would be “appropriate” for charterers and other parties in any contractual chain. One interpretation might be offered by the wording of an assured’s obligations to maintain “reasonable measures to ensure compliance with the US or UK national Cyber Security Centre recommendations or equivalent national recommendations” as contained in certain cargo clauses used in the Lloyd’s market[1]. It does seem however that whilst owners with SMS certification post-January 2021 will have a clearly defined standard against which they can be judged, the position of other parties is less certain.

[1] “CYBER COVERAGE CLAUSE JC2019-004 – for Cargo Market Joint Cargo Committee of LMA and IUA”

The second part of the clause seeks to impose an obligation on each party to use reasonable endeavours to ensure that any third parties involved in the performance of the contract also comply with the requirements set out in the first part. The parties will clearly need to look to the contractual relationships with their sub-contractors to ensure compliance with these stipulations.

The third part sets out the actions the parties should undertake if a cyber incident occurs within its own systems or if an external event is likely to affect those systems. There is a primary obligation to mitigate and, if possible, resolve the threat posed by the incident and the party must also give prompt notification of the incident to their counterparty, thereafter providing further information and advisory measures once the incident has been investigated. Importantly, each party has a continuing obligation to provide their counterparties with information that may assist them in mitigating the effect of the cyber security incident.

The final part of the clause enables the parties to agree a limit of liability to the other or accept the clause default limit of US$100,000, with the limit to apply unless liability is proven to have arisen solely from the gross negligence or wilful misconduct of the other party.

Increasing threat

The threat posed to the maritime industry from cyber attack will only increase in the short and medium terms. Deeper network integration, greater connectivity of hitherto isolated control systems and the ongoing development of autonomous shipping all greatly increase the attack surface and systems need to be hardened to mitigate the increased risks of compromise. Looking further forward there is the prospect of further challenges being posed by the as yet largely unchartered waters of artificial intelligence.

It is not possible to predict how international conventions and legislation will keep pace with this rapidly developing digitisation of the marine industry, but owners do face the immediate need to prepare their systems to satisify the next Safety Management System audit after 1 Janaury 2021.

Insurers are also becoming more demanding; cyber insurance is becoming more tailored and underwriters are requiring more (and clear) evidence that shipowners are investing in and deploying cyber security processes and technology before they will agree to provide any cyber risk cover.

Responding to these challenges and protecting marine assets from the increased threats will require investments in secure architectures and protective technologies, with expertise required to implement the new systems and to train both management and staff unfamilar with the defence against cyber risks. Elevating cyber to a more prominent position alongside safety is therefore a crucial step for the shipping industry and the key will now be to find the right balance between cost and benefit.

The BIMCO clause is the first cyber-specific clause to allocate responsibility. Whether it will be adopted by the industry remains to be seen but it represents an important pointer to helping shipowners understand operational responsibility around cyber incidents.