UK GOVERNMENT RELEASES CODE OF PRACTICE – CYBER SECURITY FOR SHIPS

On 16 June 2017, the IMO adopted Resolution MSC.428(98) which encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of shipping companies' DOCs after 1 January 2021.

It has never been more important to have effective cyber security and crisis management plans in place, as highlighted by the recent NotPetya ransomware incident which effected Maersk. Cyber attacks can harm and damage crew, vessels and cargo and

> **"It has never been more important to have effective cyber security and crisis management plans in place, as highlighted by the recent NotPetya ransomware incident which effected Maersk."**

cause business disruption, loss of sensitive information and damage to the company's image. The UK Government's new Code of Practice – Cyber Security for Ships provides further (non-binding) guidance to shipping companies, complementing last year's code of practice for ports and port systems.

During London International Shipping Week Lord Callanan, the UK Government's Transport Minister, announced the publication of the "Code of Practice – Cyber Security for Ships" (Code). Produced in conjunction with the Institute of Engineering and Technology, the UK Government's Department for Transport and the Defence Science and Technology Laboratory, this is the latest best practice guideline for the shipping industry. This code follows the UK government's cyber security code of practice for ports and port systems which was released last year. The two codes are complimentary and provide additional useful guidance to the shipping industry on how to ensure cyber preparedness.

As global IT systems have become increasingly inter-connected, so has the shipping industry. This process is set to accelerate in future as the industry looks to autonomous and semi-autonomous vessels. These vessels will require propulsion and machinery system management and emissions and ballast water monitoring from the shore, creating new opportunities for exploitation. The motivation for cyber attacks can be wide ranging, from low level cyber vandalism and hacktivism to espionage, terrorism and warfare. The shipping industry must be ready to deal with this broad range of threats.

The Code is meant to be read by all those involved in the financial and operational management of ships, from board members to senior officers including the Captain/Master, First Officer and Chief Engineer, and those responsible for the daily operation of maritime IT, operational and communications systems.

The Code makes a number of recommendations, including:

1. The development of a Cyber Security Assessment (CSA)

CSAs should be used to adopt a risk management approach to the threat posed by cyber security. They allow companies to make appropriate and proportionate investment and prioritise risks. A CSA will involve the identification of essential or sensitive assets and business processes, the possible threats facing these assets and processes, the security controls that are available and the costs of implementing them.

2. The development of a Cyber Security Plan (CSP)

A CSP should build upon the ship security plan on board a vessel. In developing a CSP, a holistic approach should be adopted, covering individuals, processes and the physical and technological aspects of a ship. Appendix C of the Code provides a useful outline. Sensitive ship systems may be protected as follows:

- Physical – Access to sensitive systems should be restricted and logs kept of those who are authorised to access those systems.
- Personnel – Administrative, engineering and technical personnel should undergo pre-employment screening and periodic background checks and should be regularly trained to ensure up-to-date cyber security awareness.
- Process – Processes should be in place to monitor and log all those who access systems.
- Technical – Measures should be in place to check removable media for malware. Consoles should be password protected.

3. CSP monitoring and review

CSPs should be reviewed at least annually to ensure that they are up to date with the latest issues facing the industry. CSPs should also be monitored periodically to ensure that they are being correctly implemented and complied with.

4. The appointment of a Cyber Security Officer (CySO)

A CySO should be responsible for all security aspects of cyber-enabled systems and for liaising with the company security officer on aspects relating to physical, personnel and process security. He should also be in charge of the development, implementation, monitoring and review of the CSP. He should be aware of any legal and regulatory changes which could impact a ship or its crew. The Code also suggests that the CySO must understand the jurisdictional issues regarding law enforcement and cyber security incidents, seeking the assistance of expert legal advice in the event of an incident.

5. The establishment of a Security Operations Centre (SOC)

The SOC is a centralised unit to deal with issues affecting the various cyber related systems on board a vessel (or a fleet of vessels) and would ordinarily be the same as the company's usual operations centre. The SOC should understand potential, emerging and actual threats faced by a vessel, take proactive steps where possible to minimise a threat and handle any security breaches and incidents.

6. A plan to deal with security breaches and incidents

The CySO and SOC must have an effective crisis management plan in place to handle a cyber incident. Appendix D of the Code provides a basic framework. If a vessel or company's IT system is compromised it could lead to harm and damage to crew, vessels and cargo, business disruption, loss of sensitive information and damage to the company's image. The crisis management plan should also be tested and reviewed regularly both internally and with external advisors with the necessary skills and expertise. Systems and processes should also be developed for the handling and release of sensitive data.

It is recommended that Ship owners should review the terms and conditions of their contracts with their suppliers, insurers and other important third parties. It is likely that certain interests will try to impose the requirement to comply with the Code or include warranties. It is also possible that compliance with the Code will become a requirement of doing business with certain third parties. For example, companies wishing to bid for UK Government contracts are now required to be Cyber Essentials certified.

The Code provides further useful (non-binding) guidance on cyber security and has much in common with the Guidelines on Cyber Security On board Ships produced by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI. Whichever of the industry-recognised guidelines on cyber security any shipping company chooses to adopt, it is advisable that it actively addresses issues of cyber security. It is considered that it is only a matter of time before being unable to demonstrate the exercise due diligence in managing cyber risks may lead to loss of contractual defences and/or insurance cover in the event of loss arising from a cyber incident.

A link to the Code can be found at http://www.hfw.com/New-BIMCO-Guidelines-July-2017. For more information on developing your cyber resilience and crisis management plan, please contact:

TOBY STEPHENS
Partner, Singapore
T +65 6411 5300
E toby.stephens@hfw.com

ELECTRA PANAYOTOPOULOS
Partner, Piraeus
T +30 210 429 3978
E electra.panayotopoulos@hfw.com

PETER SCHWARTZ
Consultant, London
T +44 (0)20 7264 8171
E peter.schwartz@hfw.com

HFW has over 500 lawyers working in offices across Australia, Asia, the Middle East, Europe and the Americas. For further information about our shipping capabilities, please visit hfw.com/shipping

hfw.com

Beirut Brussels Dubai Geneva Hong Kong Houston Kuwait London Melbourne Paris Perth Piraeus Riyadh São Paulo Shanghai Singapore Sydney