Cyber security on board ships - Tanker Management and Self Assessment and upcoming changes to the International Safety Management Code

On 1 January 2018, the Oil Companies International Marine Forum's (OCIMF) Tanker Management and Self Assessment (TMSA) version 3 will come into force. The TMSA programme provides companies with a means to improve and measure their own safety management systems.

One of the salient changes in the TMSA version 3 is the addition of the 13th performance element which focuses on Maritime Security. This new element will require Members who are subscribed to the Ship Inspection Reporting Programme (SIRE) programme, to incorporate cyber risk security policies and procedures within the company/vessel's operating procedures. To be more specific, operators will be required to have:

- procedures on software management
- guidance on how to identify and mitigate cyber threats
- availability of latest guidelines on cyber security from industry and classification society
- password management procedures
- and a cyber security plan which can be shared with staff to promote cyber awareness on board.

Further details regarding the TMSA 3 can be found on the Oil Companies International Marine Forum website.

Whilst the International Maritime Organization (IMO), by way of the Maritime Safety Committee's 98th session in June 2017, adopted Resolution MSC.428(98) which allows owners and operators until 1 January 2021 to incorporate cyber risk management systems as per the International Safety Management (ISM) Code, the OCIMF have determined that more immediate action is necessary by implementing cyber compliance requirements via the TMSA version 3.

Further guidance and information on cyber security can be obtained from our articles ISM – Cyber Security, Be Cyber aware at Sea, Cyber Guidance for Crews and Cyber security guidelines for vessels.

The IMO has also published *Guidelines on Maritime Cyber Risk Management* which may also be consulted for further reference.

If Members require further assistance, please contact the Loss Prevention team.