MyriadSea

Management System

FLEET DIRECTIVE

FD-01-2021

18 July 2021

SMMS Update

MSMS has been updated to include instructions and procedures for Cyber Security management. These new instructions are effective immediately. For those accessing MSMS online, the change is already reflected in the system (you may need to refresh your browser).

For those accessing a local version, an update will be issued shortly – in the meantime, a copy of the new procedure is attached here.

Nature of the change(s):

- Section C07 Cyber Security added

Please ensure this directive is shared widely, and all take the time to become familiar with the new section.

Ian McIntosh-Oakley
Managing Director

C07
Cyber Security

Version 01, Issue Date 18.07.2021

07.1 General

Ships are increasingly using systems that rely on digitisation, integration, and automation, which calls for cyber risk management on board.

As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together and more frequently connected to the internet.

This brings the greater risk of unauthorised access or malicious attacks to ships' systems and networks.

Risks may also occur from personnel accessing systems onboard, for example by introducing malware via removable media.

Cyber security and safety management Cyber safety is as significant as cyber security. Both have equal potential to affect the safety of onboard personnel, ships, and cargo. Cyber security is concerned with the protection of IT and data from unauthorized access, manipulation and disruption. Cyber safety covers the risks from the loss of availability or integrity of safety critical data.

Cyber safety incidents can arise as the result of:

- A cyber security incident, which affects the availability and integrity of OT, for example corruption of chart data held in an Electronic Chart Display and Information System (ECDIS)
- A failure occurring during software maintenance and patching
- Loss of or manipulation of external sensor data, critical for the operation of a ship.

This includes but is not limited to Global Navigation Satellite Systems (GNSS).

Whilst the causes of a cyber safety incident may be different from a cyber security incident, an effective response to both is based upon training and awareness.

07.2 Background

In June 2017, the IMO’s Maritime Safety Committee (MSC) took a significant step forward in combating the threats posed by cyber risks to the safety and security of personnel ashore and on ships.

In June 2016, the MSC had introduced “high level recommendations for maritime cyber risk management” in the form of interim guidelines. These were designed to provide overarching direction for the shipping industry, and all its stakeholders, in the management of the risks posed by both unintentional and malicious acts against the cyber infrastructure of an organisation.

In 2017 the MSC agreed to adopt a resolution incorporating Maritime Cyber Risk Management into the ISM Code, thereby raising the profile and importance of protecting ships, crews and cargos from the threats of accidental cyber-related incidents and premediated cyber-attacks.
The MSC are encouraging all members to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company’s Document of Compliance (DOC) after 1st January 2021.

07.3 Relevant Cyber Security Areas

Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment.

In some cases, these systems are to comply with international standards and Flag Administration requirements. However, the vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to:

.1 Bridge systems;
.2 Cargo handling and management systems;
.3 Propulsion and machinery management and power control systems;
.4 Access control systems;
.5 Passenger servicing and management systems;
.6 Passenger facing public networks;
.7 Administrative and crew welfare systems; and
.8 Communication systems.

On our ships, the following systems are relevant:

.1 Bridge systems;
.2 Cargo handling and management systems;
.3 Propulsion and machinery management and power control systems;
.7 Administrative and crew welfare systems; and
.8 Communication systems.

In our shore based locations, the following systems are relevant:

- Communication systems

Failures of these systems can have a significant impact on the operation of the vessel.

07.4 Responsibilities

The Managing Director is responsible for cyber security across the business. He may delegate operational responsibility to any other suitable employee.

Onboard, operational responsibility for cyber security rests with the Master.

All personnel have are responsible for the identification of cyber security threats.

07.5 Critical Systems

In priciple, critical systems are those defined elsewhere in this system. They are the systems required for the safe operation of the vessel and include propulsion, navigation and emergency response systems.

The approach to risk assessment for critical systems is the same as any other cyber risk, however the critical nature of the system can mean that the impact of the risk actually happening can be more severe. This should be reflected in the response measures.

07.6 Threat Identification, Risk Assessment, Measures

Threats have been assessed in each of the relevant risk areas for the business. The company's standard risk assessment process has been used for this purpose. It is important to recall that any risk assessment is based on a "point in time" review. If circumstances change, the risk or response may need to be adapted.

For each threat, an assessment has been carried out and required actions identified.

Bridge & Communications Systems

There are no bridge operational systems on our vessels continuously connected to the internet. However, a number of key systems rely on internet or email based updates to continue operating safely.

ECDIS

ECDIS relies on email updates to remain updated and safe for use. ECDIS is a critical system, as it is the primary means of navigation for our fleet.

Risks:
- Introduction of malicious software through a regular update file (either intentionally, or through the use of an affected USB drive or disc).
- Introduction of malicious software by a service technician

Current mitigation measures:
- One dedicated USB stick used for all ECDIS updates
- All ECDIS updates are received from a single official source
- ECDIS updates are received on a fixed schedule from the official source
- Only manufacturers authorised technicians are authorised to carry out work on the system

Risk Assessment: **Moderate**
Probability: Low - The ECDIS system is largely isolated from connected systems, and updates are received only from a single official source
Impact: Severe - Loss of the ECDIS system could severely impact safe navigation

Further Actions Required:
- NIL

Communications Systems

No GMDSS systems within the fleet are connected directly to the internet. Normal operational communications are carried out on a single computer, using a commercially available satellite system.

Risks:
- Introduction of malicious software through the use of an infected USB drive (most likely unintentionally)
- Failure of the satellite communications system

Current mitigation measures:
- Antivirus software kept up to date on the main comms computer
- Communication system has integrated firewalls maintained by the manufacturer
- Standard software used for connectivity, enabling the computer to be interchanged
- GMDSS systems allow for communication by other means in the event of a failure of the main system (eg. Sat-C)

Risk Assessment: Moderate
Probability: Moderate - There is a moderate chance of a person using an infected drive
Impact: Moderate - There are alternative means of ensuring ongoing essential communication until the next port

Further Actions Required:
- NIL

Cargo Handling Systems

There are currently no connected cargo handling systems on our vessels. Cargo cranes have control software however.

Cargo Cranes

The cargo cranes utilise control software and systems

Risks:
- Introduction of malicious software by a service technician

Current mitigation measures:
- Only manufacturers authorised technicians are authorised to carry out work on the system

Risk Assessment: Low
Probability: Very Low - The system is largely non-connected
Impact: Low - The fleet can operate safely without cargo cranes

Further Actions Required:
- NIL

Propulsion and Machinery Management and Power Control Systems

There are no connected machinery or propulsion control systems on the vessel. The systems themselves are separate from general working computers, and have no usable operating system beyond their primary purpose.

Machinery Control Systems

These systems are not connected, and can only be accessed by authorised technicians.

Risks:
- Introduction of malicious software by a service technician

Current mitigation measures:
- The systems (beyond normal use) can only be accessed by an authorised technician
- Ship staff have no access to passwords for access
- There is no additional "operating system" for these computers

Risk Assessment: Low
Probability: Very Low
Impact: Severe

Further Actions Required:
- NIL

Administrative & Crew Welfare Systems

The vessels in the fleet have crew internet access on a BYOD Bring Your Own Device basis, using a commercial satellite system, which also includes a welfare channel for entertainment. There is a shipboard administration network for use in day to day business.

Crew Internet Access
The crew internet system uses the same communications satellite network as the main ships business communication system.

Risks:
- Introduction of malicious software through the use of an infected device
- Failure of the satellite communications system
- Access to (or loss of) ships data as a result

Current mitigation measures:
- Key onboard data is routinely replicated or sent ashore (at least monthly) to ensure a backup of recent data available
- Satellite provider includes additional firewall and antivirus protections for crew access to onboard internet (i.e. login to a crew account has additional requirements)
- Other communications systems are available to enable ship to reach next port safely
- Only ship staff are permitted to access the internet onboard - external parties and internal shore staff are not granted access

Risk Assessment: **Moderate**
Probability: Moderate
Impact: Moderate

Further Actions Required:
- NIL

Onboard Administration Network
The ships business network is wireless, using the same access points as crew and business internet.

Risks:
- Introduction of malicious software through the use of an infected device (intentional or not)
- Access to (or loss of) ships data as a result

Current mitigation measures:
- Key onboard data is routinely replicated or sent ashore (at least monthly) to ensure a backup of recent data available

Risk Assessment: Moderate
Probability: High
Impact: Moderate

Further Actions Required:
- External parties and shore staff are not to be permitted to access or use the ships network. Where external parties need to print documents, the documents must be sent by email to the ship or printed on a completely network isolated printer.

ASHORE

Shore-Based Communication Systems
The company has no fixed IT infrastructure ashore. All IT systems are cloud-based, from Microsoft and Amazon.

Shore Based Systems

The company uses Office365 for most work, and Amazon Workspaces to access the Planned Maintenance System SMMS (hosted in the cloud).

Risks:
- Unauthorised Access to company systems
- Cloud provider unable to provide services

Current mitigation measures:
- Multi-Factor authentication is in use on all company systems
- Telephone communications are always available and independent of IT systems

Risk Assessment: Low
Probability: Low - the company uses external providers with high quality security systems
Impact: Moderate

Further Actions Required:
- NIL

07.7 Threat Management Actions

The effectiveness of actions depends entirely on how well or not they are implemented. The Company madates the actions required, it is the responsibility of the Master to ensure they are in fact in place.

If for any reason an action or actions cannot be properly implemented, the Master must inform the Ship Management Team immediately.

07.8 Regular Review of Threats and Measures

Threats and measures are to be reviewed:
- Every year, or
- Whenever a new digital system is installed onboard, or
- Whenever a new threat is identified, or
- Whenever there is a reason to suspect that the measures may no longer be effective

Whichever is shorter.

07.9 Response to a Cyber Security Event

Should a cyber security event occur or be anticipated, the Shore Emergency Team will meet.

Contact is to be made with the ship in question, and a response plan put in place. The response is to prioritise:
- Safety of the vessel and crew
- Safety of the marine environment
- Cargo interests
- Operational interests

In descending order of priority.

The Company must consider which partners should be brought into the response. These could include:
- IT Service Providers (for example Can Traders Singapore)
- IT Security Consultants (for example Control Risks)
- Class (for example BV)
- Flag
- Agents
- Cargo Interests

The event response is to continue until the Managing Director confirms otherwise.

07.10 Training

The Company is to identify cyber security training needs for crew and shore based personnel as part of the normal training needs identification process.