Maritime cybersecurity using ISPS and ISM codes

Alejandro Gómez Bermejo
Cybersecurity Manager and Consultant
BEng, PMP, CISA, CRISC, ITIL, AMNI, Yachtmaster
www.erawat.es

Introduction

Currently neither the IMO nor the national authorities have regulated on incorporating cybersecurity controls in the maritime sector.

In this article I present some ideas to incorporate maritime cybersecurity policies, procedures and controls in vessel operations.

First, I make a brief description of the IMO security ISPS and safety ISM codes. Then, I indicate how cybersecurity could be incorporated using these codes.

ISPS code. Security of ships and port facilities.

The guidelines for preventing deliberate attacks on ships and port facilities is defined in the International Ship and Port Facility Security Code ISPS adopted by the IMO International Maritime Organization in 2002.

The ISPS code applies to ships engaged on international voyages including passenger ships and cargo ships over 500 gross tonnage. The code does not does not apply to naval ships or Government ships used on non-commercial service.

The ISPS code comprises a first part (A) of mandatory provisions and a second part (B) of optional provisions at the discretion of national authorities.

The ISPS has been enforced in the European Union by EC regulation 725/2004 confirming as compulsory the provisions in part A and some of provisions in part B.

The objectives of the ISPS code are:

- Establish an international framework involving co-operation between Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade.
- Establish the respective roles and responsibilities of the Governments, Government agencies, local administrations and the shipping and port industries, at the national and international level for ensuring maritime security.

- Ensure the early and efficient collection and exchange of security-related information.
- Provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels.
- Ensure confidence that adequate and proportionate maritime security measures are in place.

The threats considered in the ISPS Code are mainly of physical type. Ships are required to apply incremental protective security measures according to the following levels:

- Security level 1: level for which minimum appropriate protective security measures shall be maintained at all times.
- Security level 2: level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.
- Security level 3: level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

The ISPS contracting national governments are responsible for the following:

- Setting of the applicable security level.
- Approving a Port Facility Security Assessment and subsequent amendments to an approved assessment.
- Determining the port facilities which will be required to designate a Port Facility Security Officer.
- Approving a Port Facility Security Plan and subsequent amendments to an approved plan.
- Exercising control and compliance measures..
- Establishing the requirements for a Declaration of Security.

Ship Security Plans in ISPS

According to the ISPS code a ship security plan SSP needs to be created. The organization and procedures of the ship security plans SSP should establish:

- The duties and responsibilities of all shipboard personnel with a security role.
- The procedures or safeguards necessary to allow such continuous communications to be maintained at all times.
- The procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction.

- The procedures and practices to protect security sensitive information held in paper or electronic format.
- The type and maintenance requirements, of security and surveillance equipment and systems, if any.
- The procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns.
- The procedures to establish, maintain and up-date an inventory of any dangerous goods or hazardous substances carried on board, including their location.

The SSP is clearly focused on physical security. For example, its contents will include references to people responsibilities on the ship and on land, physical access controls to the ship, guards and patrols, CCTV surveillance and prevention and action against possible pirate attacks.

An example of the recommended content for the SSP (USCG) is shown below:

- Security organization of the vessel
- Personnel training
- Drills and exercises
- Records and documentation
- Response to change in MARSEC Level
- Procedures for interfacing with facilities and other vessels
- Declarations of Security (DoS)
- Communications
- Security systems and equipment maintenance
- Security measures for access control, including designated passenger access areas and employee access areas
- Security measures for restricted areas
- Security measures for handling cargo
- Security measures for delivery of vessel stores and bunkers
- Security measures for monitoring
- Security incident procedures
- Audits and Vessel Security Plan (VSP) amendments
- Vessel Security Assessment (VSA) report.

ISM code. Safe operation of ships.

The guidelines for the safe operation of ships are defined in the IMO International Safety Management ISM code. This code was originally approved by IMO in 1993 and was made mandatory from 1998.

The ISM Code applies to passenger ships irrespective of their tonnage and cargo ships over 500 gross tonnage. It does not apply to vessels of non-commercial use.

The objectives of the ISM Code are to ensure safety at sea, prevention of human injury or loss of life, and avoidance of damage to the environment, in particular to the marine environment and to property.

According to the ISM code, the safety management objectives of the shipping company should:

- Provide for safe practices in ship operation and a safe working environment.
- Assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards.
- Continuously improve safety management skills of personnel ashore and aboard ships, including preparing for emergencies related both to safety and environmental protection.

Every shipping company should develop, implement and maintain a safety management system SMS which includes the following functional requirements:

- A safety and environmental-protection policy.
- Instructions and procedures to ensure safe operation of ships and protection of the environment in compliance with relevant international and flag State legislation.
- Defined levels of authority and lines of communication between, and amongst, shore and shipboard personnel;
- Procedures for reporting accidents and non-conformities with the provisions of this Code;
- Procedures to prepare for and respond to emergency situations.
- Procedures for internal audits and management reviews.

Safety Management Manual in ISM

The operation of the safety management system SMS must be documented and each ship should carry on board all documentation relevant to that ship.

The documents used to describe and implement the safety management system may be referred to as the Safety Management Manual SMM.

The SMM manual is focused on the safety of operations, people and the environmen. An example of the recommended content for the SMM manual (USCG Vessel safety program) is shown below:

- Introduction
- Safety and Environmental Protection Policy
- Company Responsibility and Authority

- Designated Persons
- Master's Responsibility
- Resources and Personnel
- Vessel Operating Procedures
- Emergency Preparedness
- Reporting Procedures
- Maintenance
- Documentation
- Company Verification and Review

Maritime cybersecurity on ships

Some safety management manuals SMM include references to information systems security on board. However, these references to information security or computer security are usually very basic.

For example, the SMM will refer to the security measures of onboard computer systems such as protection with passwords, performing backups and protection of the equipment containing the SMM manual.

The SSP manual will normally have a strong focus on physical security.

SMM and SSP manuals will rarely include cybersecurity policies, controls or procedures.

In my opinion, the Ship Security Plan SSP and Safety Management Manual SMM may be the appropriate documents to include references to maritime cybersecurity policies and controls such as:

- Risk analysis of information technology IT systems
- Preventive security measures deployed in the ship and ashore to mitigate risks in IT systems to an acceptable level.
- Internet access security policy indicating restrictions applicable depending on the operations being performed on the ship.
- Policy for the use of removable storage media such as usb sticks, external drives, CDs and DVDs.
- Policy and network access controls for the crew and wireless WiFi networks.
- Policy and procedures for updating and maintaining information and navigation systems.
- Physical and logical access controls to the various ship systems based on its sensitivity level.
- Authorization criteria for remote connections from the company office for system monitoring and maintenance.
- Contingency plan for information technology IT systems.

- Cyberincident management procedures: detection, reporting, assessment and decision, response, recovery and lessons learned.
- Training and awareness of master, officers, engineers and crew on cybersecurity risks and controls.

For example, a maritime cybersecurity policy should require disabling or limiting access to Internet and WiFi connections during sensitive operations such as port approaches, piloting and berthing operations.

Cybersecurity manual and procedures

Cybersecurity manuals, procedures and checklists should have their own identity and the supporting documentation should be incorporated in a Ship Cybersecurity Manual (MCSEC).

The MCSEC could be referred from the SSP and SMM as in the following examples:

- The existence of a contingency plan for the ECDIS navigation systems should be in the SMM. In case there is a contingency, the details of the IT Systems Contingency Plan, including ECDIS, should be found in the MCSEC.

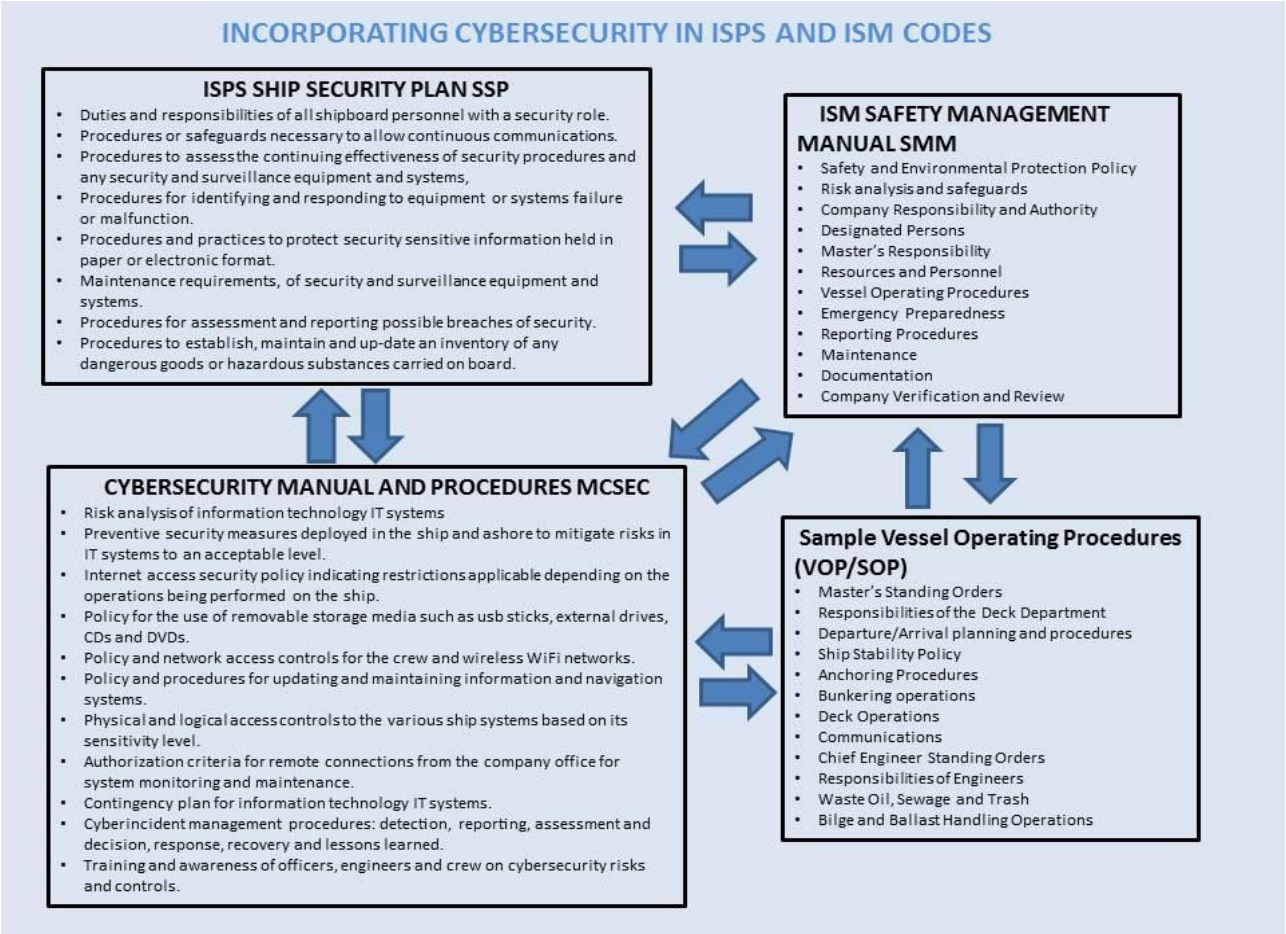
- Physical access control to different areas of the ship should be indicated in the SSP. Logical access controls for IT systems in the different physical areas should be found in the MCSEC.

- Ship position readings in ECDIS do not correspond with previous ECDIS readings or current visual fixes suggesting a system malfunction or deliberate interception. Besides following SMM recommended procedures for the safe navigation of the ship, the MCSEC cyberincident management procedure should be consulted to assess the potential cyberincident and respond appropriately.

It is very important to realize that the definition and documentation of the MCSEC manual and policies is only a first step.

It is also necessary to deploy the cybersecurity procedures, controls and checklists, provide training, test regularly and verify the results in order to improve.

Below I present a high-level diagram showing how some of the elements required by ISPS and ISM could interact with maritime cybersecurity policies and procedures.



Acronyms:

- ISPS: International Ship and Port Facility Security
- ISM: International Safety Management
- SSP: Ship Security Plan
- SMM: Safety Management Manual
- MARSEC: Maritime Security
- ECDIS: Electronic Chart Display and Information System
- MCSEC: Cybersecurity Manual

References:

- ISPS code IMO: http://www.imo.org/OurWork/Security/Guide_to_Maritime_Security
- ISM code IMO: http://www.imo.org/OurWork/HumanElement/SafetyManagement
- USCG Vessel Security Plan: http://www.gpo.gov/fdsys/pkg/CFR-2010-title33-vol1/pdf/CFR-2010-title33-vol1-sec104-405.pdf
- USCG Vessel safety program: http://www.uscg.mil/pvs/SPV.asp