IET Standards

[dstl]

Department for Transport

Code of Practice

Cyber Security for **Ships**

Publication Information

Authors: Hugh Boyes and Roy Isbell

The IET would like to acknowledge the help and support of Department for Transport (DfT) and Defence Science and Technology Laboratory (Dstl) in producing this Code of Practice.

Published by: Institution of Engineering and Technology, London, United Kingdom

The Institution of Engineering and Technology is registered as a Charity in England & Wales (no 211014) and Scotland (no SC038698).

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR
Telephone 0300 330 3000
General enquiries https://forms.dft.gov.uk
Website www.gov.uk/dft

ISBN 978-1-78561-577-1 (paperback)

CONTENTS

Foreword

This Code of Practice should be read by board members of organisations with one or more ships, insurers, ships' senior officers (for example, the Captain/Master, First Officer and Chief Engineer) and those responsible for the day-to-day operation of maritime information technology (IT), operational technology (OT) and communications systems. It does not set out specific technical or construction standards for ship systems, but instead provides a management framework that can be used to reduce the risk of cyber incidents that could affect the safety or security of the ship, its crew, passengers or cargo.

The maritime sector is a vital part of the global economy, whether it is carrying cargo, passengers or vehicles. Ships are becoming increasingly complex and dependent on the extensive use of digital and communications technologies throughout their operational life. Poor security could lead to significant loss of customer and/or industry confidence, reputational damage, potentially severe financial losses or penalties, and litigation affecting the companies involved. The compromise of ship systems may also lead to unwanted outcomes, for example:

(a) physical harm to the system or the shipboard personnel or cargo – in the worst case scenario this could lead to a risk to life and/or the loss of the ship;
(b) disruptions caused by the ship no longer functioning or sailing as intended;
(c) loss of sensitive information, including commercially sensitive or personal data; and
(d) permitting criminal activity, including kidnap, piracy, fraud, theft of cargo, imposition of ransomware.

The above scenarios may occur at an individual ship level or at fleet level; the latter is likely to be much worse and could severely disrupt fleet operations.

Cyber security is not just about preventing hackers gaining access to systems and information, potentially resulting in loss of confidentiality and/or control. It also addresses the maintenance of integrity and availability of information and systems, ensuring business continuity and the continuing utility of digital assets and systems. To achieve this, consideration needs to be given to not only protecting ship systems from physical attack, force majeure events, etc., but also to ensuring the design of the systems and supporting processes is resilient and that appropriate reversionary modes are available in the event of compromise. Personnel security aspects are also important. The insider threat from shore-based or shipboard individuals who decide to behave in a malicious or non-malicious manner cannot be ignored. Ship owners and operators need to understand cyber security and promote awareness of this subject to their stakeholders, including their shipboard personnel.

This Code of Practice explains why it is essential that cyber security be considered as part of a holistic approach throughout a ship's lifecycle, as well as setting out the potential impact if threats are ignored. The Code of Practice is intended to be used as an integral part of a company's or ship's overall risk management system and subsequent business planning, so as to ensure that the cyber security of the ship, or fleet, is managed cost effectively as part of mainstream business.

Terms and definitions

Definitions used in this Code of Practice are, to the extent practicable, in keeping with those contained in the International Convention for the Safety of Life at Sea, 1974, (SOLAS) as amended. For ease of reference, certain terms used in this document are defined below.

Asset
Item, thing or entity that has potential or actual value to an organization.

[BS ISO 55000:2014, **3.2.1**]

Asset information
Data or information relating to the specification, design, construction, acquisition, operation or maintenance of an item, thing or entity that has potential or actual value to an organization. This also includes its disposal or decommissioning. It can include design information and models, documents, images, software, spatial information and task or activity-related information.

Company
The owner of the ship or any other organisation or person, who has assumed responsibility for the operation of the ship from the owner of the ship, and who on assuming such responsibility, has agreed to take over the duties and responsibilities imposed by the International Safety Management (ISM) Code.

[International Ship and Port Facility Security (ISPS) Code, Section 1.8, p.10]

Company security officer (CSO)
The person designated by the Company for ensuring that a Ship Security Assessment (SSA) is carried out, that a ship security plan (SSP) is developed, submitted for approval, and thereafter implemented and maintained, and for liaison with port facility security officers (PFSOs) and the ship security officer (SSO).

[ISPS Code, Section 1.8, p.10]

Cyber-physical system (CPS)
System designed as an entity, or set of entities, with a specific purpose, or to meet a capability objective. A CPS should include a computational aspect (cyber) and a physical aspect working together to accomplish a task or function. The cyber aspect has a controlling or influencing role over the physical parts of the system, for example, the automated steering of a ship to maintain a planned course.

Cyber security officer (CySO)
The person or persons tasked to manage and coordinate the cyber security of a ship. For larger fleets the CySO is likely to report to the Company's Chief Information Security Officer (CISO) or CSO, for smaller fleets the role is likely to report to the Company's Head of Security.

High risk position
A position that has access to the details of the SSA, SSP, CSP and/or information relating to sensitive assets, a position that fulfils an IT, OT or Communications system administrative function or information management role.

Non-SOLAS ship
A ship to which the SOLAS Convention does not apply.

[ISPS Code, Section 1.8, p.11]

Operational technology (OT)
The technology commonly found in cyber-physical systems that is used to manage physical processes and actuation through the direct sensing, monitoring and or control of physical devices, for example, motors, valves, pumps, etc. In a vessel these systems include: plant and machinery, RF communications, on and off board sensors and navigation systems.

Personnel
Individuals employed by an organization, including contractors or temporary staff used to fulfil roles that may be undertaken by that organization.

Port
The geographical area defined by the Member State or the designated authority, including port facilities as defined in the ISPS Code, in which maritime and other activities occur.

[ISPS Code, Section 1.8, p.11]

Note: Whilst this definition applies to an area, which may be enclosed within a physical boundary for the purposes of physical security, from a cyber security perspective the port will include the port systems wherever they may be located, for example, hosted in a remote data centre.

Risk appetite
A function of an organization's capacity to bear risk.

Security incident
Any suspicious act or circumstance threatening the security of a ship or of a port facility or of any ship/port interface or ship-to-ship interface.

[ISPS Code, Section 1.8, p.12]

Note: This includes cyber security incidents.

Security level
The qualification of the degree (probability and impact) of risk that a security incident will be attempted or will occur.

[ISPS Code, Section 1.8, p.12]

- **Security level 1**

The level for which minimum appropriate protective security measures shall be maintained at all times.

[ISPS Code, Section 1.8, p.12]

- **Security level 2**

The level for which appropriate additional protective security measures shall be maintained at all times.

[ISPS Code, Section 1.8, p.12]

- **Security level 3**

The 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.

[ISPS Code, Section 1.8, p.12]

Security-sensitive information
Information, the disclosure of which would compromise the security of the ship, including, but not limited to, ship operational data, information contained in any personnel-related file or privileged or confidential information that would compromise any person, system or organisation.

Sensitive asset
An asset – as a whole or in part – that may be of interest to a threat actor for hostile, malicious, fraudulent and/or criminal behaviour or activities.

Sensitive information
Information, the loss, misuse or modification of which, or unauthorised access to, could:

(a) adversely affect the privacy, welfare or safety of an individual or individuals;
(b) compromise intellectual property or trade secrets of an organization;
(c) cause commercial or economic harm to an organization or country; or
(d) jeopardise the security, internal and foreign affairs of a nation, depending on the level of sensitivity and nature of the information.

Sensitive ship systems
These systems will vary according to the type and function of a ship, but are likely to include:

(a) critical systems;
(b) systems required for the safety of life and safe operation of the vessel;
(c) systems holding personal information; and
(d) the VDR.

Ship
A passenger ship carrying more than 12 passengers or a cargo ship engaged in an international voyage, and includes high-speed craft and mobile offshore drilling units (MODUs). Generally the provisions of the SOLAS Convention apply to cargo ships of, or over, 500 gross tonnage (gt). The Maritime Security Measures apply to passenger ships, as above, and to cargo ships over 500gt.

[ISPS Code, Section 1.8, p.12]

Note: European Commission (EC) Regulation No 725/2004 dated 31 March 2004 extends the ISPS provisions to Class A passengers operations as defined in Article 4 of European Council Directive 98/18/EC dated 17 March 1998.

Shipboard personnel
The master and the members of the crew or other persons employed or engaged in any capacity on board a ship in the business of that ship, including high-speed craft, special purpose ships and mobile offshore drilling units not on location.

[ISPS Code, Section 1.8, p.12]

Ship assets
All ship data, ship facilities and ship systems.

Ship data
Any data, information, models and processes associated with the ownership, design and operation of a ship.

Ship/port interface
The interactions that occur when a ship is directly and immediately affected by movements involving the movement of persons, goods or the provisions of port services to or from the ship.

[ISPS Code, Section 1.8, p.12]

Ship security alert system (SSAS)
The means by which a ship can transmit a security alert to a competent authority on shore, indicating that the security of the ship is under threat or has been compromised.

[ISPS Code, Section 1.8, p.12]

Ship security assessment (SSA)
A risk assessment undertaken by, or for, a company security officer as a prelude to the preparation of a ship security plan or the review, or amendment, of an approved ship security plan.

[ISPS Code, Section 1.8, p.12]

Note: MCA Guidance to Surveyors states: "The SSA must be carried out by properly trained personnel. This includes those who have attended approved Company Security Officer and Ship Security Officer courses and may include classification societies or reputable firms of consultants. The UK is not approving Recognised Security Organisations (RSO), therefore any reputable firm of consultants may be utilised to carry out the SSA. There must be evidence that the Company has accepted the SSA."

Ship security officer (SSO)
The person on board the ship, accountable to the master, who is designated by the Company as responsible for security of the ship, including implementation and maintenance of the ship security plan, and for liaison with the company security officer and port facility security officers.

[ISPS Code, Section 1.8, p.12]

Ship security plan (SSP)
A plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

[ISPS Code, Section 1.8, p.12]

Ship systems
Systems that are used to manage or control the cyber-physical systems on a ship which may include: access control systems; management systems; goods handling systems; energy management systems; propulsion and navigation systems; fire, communications, safety and security systems; and those used to manage the ship's business.

Ship-to-ship activity
Any activity not related to a port facility that involves the transfer of cargoes, goods or persons from one ship to another.

[ISPS Code, Section 1.8, p.12]

SOLAS Convention
The International Convention for the Safety of Life at Sea, 1974, as amended.

[ISPS Code, Section 1.8, p.12]

Threat
A potential cause of an incident or hazardous situation that may result in harm to an asset, person, system or organization.

Vulnerability
A weakness (for example, systematic, procedural, physical or technical) of an asset, or group of assets, that can be exploited by one or more threats.

Acronyms

CCTV – Closed circuit television
CiSP – Cyber Information Sharing Partnership (UK)
CoP – Code of Practice
CPS – Cyber-physical system
CSA – Cyber security assessment
CSO – Company security officer
CSP – Cyber security plan
CySO – Cyber security officer
DDoS – Distributed denial of service
DfT – Department for Transport
Dstl – Defence Science & Technology Laboratory (UK)
EDi – Electronic data interchange
FSC – Fleet security committee
GNSS – Global navigation satellite system
GPS – Global positioning system
IET – Institution of Engineering and Technology
ILO – International Labour Organization
IMO – International Maritime Organization
ITU – International Telecommunications Union
ISPS – International ship and port facility security
MODU – Mobile offshore drilling units
NCSC – National Cyber Security Centre (NCSC)
OT – Operational technology
PMR – Personal mobile radios
SCADA – Supervisory control and data acquisition
SOC – Security operations centre
SOLAS – International Convention on the Safety of Life at Sea
SSAS – Ship security alert system
SSA – Ship security assessment
SSO – Ship security officer
SSP – Ship security plan

SECTION 2

Introduction

This Code of Practice considers the cyber security requirement for ships whether underway, moored or berthed, advocating a coherent, ship – or fleet – wide approach. It is intended to complement the ship security standards and their respective requirements, by providing additional guidance on the cyber-related aspects of the security measures set out. It therefore makes extensive reference to, and assumes knowledge of, the definitions and concepts contained within these regulations.

This Code of Practice uses principles rather than national legislation or specific standards to help promote good practice. However, the specific cyber security measures implemented should depend on the profile of the ship, its use and the nature of the cargoes handled.

The rapid evolution in the use of, and reliance upon, digital (computer-based) and communication technologies, as well as the advances in automation and the potential for integration of multiple electronic systems supporting management functions and business applications, increases the importance of addressing inherent vulnerabilities. It is therefore vital that ship owners, operators and masters understand and implement appropriate and proportionate measures to address the resilience and cyber security issues that arise. Only by doing so can they fully meet their responsibilities for the secure and safe operation of their ships.

While this Code of Practice is concerned solely with the cyber security of ships, it recognises that, with a large proportion of security breaches caused by people and poor processes, it is essential that personnel, process and physical aspects directly related to these technological maritime systems are also considered and appropriate measures put in place. Recommendations relating to these aspects are therefore detailed throughout the Code of Practice where relevant.

With the exception of any ship/port interface, it is not the purpose of this Code of Practice to consider the cyber security of the ports and port facilities to which the ISPS Code also applies. The UK Department for Transport (DfT) published separate guidance on ports and port systems during 2016[1].

2.1 Who should use this Code of Practice?

This Code of Practice is intended for use by those with responsibility for protecting the ships (both when underway and when docked or berthed), persons, cargo, cargo transport units and ship's stores from the risks of a security incident. It will also be of interest and relevance to those individuals involved in:

1 Code of Practice: Cyber Security for Ports and Port Systems https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice

(a) the financial and operational management of a ship or fleet;
(b) insuring ships and their cargoes;
(c) contractual arrangements with third parties;
(d) determining policies relating to acceptable staff behaviour;
(e) the specification, design, construction and maintenance of ships;
(f) the specification, design, development, integration, commissioning, operation and maintenance of maritime systems, including associated software and technologies; and
(g) management of specific security tasks, including incident response and the handling of security breaches.

2.2 Maritime Security Regulations in the UK

In December 2002 the International Maritime Organisation (IMO) adopted a series of changes to the SOLAS Convention (Safety of Life at Sea Convention) that introduced the International Code for the security of Ships and Port Facilities, more commonly referred to as the International Ship and Port Facility Security (ISPS) Code. The ISPS Code was incorporated into EU Law by the European Commission (EC) Regulation 725/2004.

For convenience the following documents are collectively referred to in this Code of Practice as the "ship security standards":

(a) ISPS Code;
(b) EC Regulation 725/2004;
(c) The Ship and Port Facility (Security) Regulations 2004 (SI 2004 No. 1495);
(d) The Port Security Regulations 2009 (SI 2009 No. 2048); and
(e) UK Ship Safety Instructions (published by the UK Department for Transport).

Note 1: The Aviation & Maritime Security Act 1990 also has some persisting relevance and can be used alongside ISPS, EC and UK legislation.

Note 2: In June 2016, the IMO issued MSC.1/Circ.1526 "Interim guidelines on maritime cyber risk management", discussions at the IMO MSC 98th session in June 2017 may result in this may form part of a new MSC Resolution.

The Maritime Security Regulations place legal requirements on the Company of a ship covered by the SOLAS Convention to put in place a Company Security Officer (CSO), who is responsible on behalf of the Company for preparation of the SSA and CSA. Section 8 of the ISPS Code requires the SSA to encompass the ship's radio and telecommunications systems, including computer systems and networks. The Company should ensure appropriate governance arrangements are in place regarding the roles and duties of the CSO and the Cyber Security Officer (CySO).

2.3 Terms and definitions

Definitions used in this Code of Practice are, to the extent practicable, in keeping with those contained in the International Convention for the Safety of Life at Sea, 1974, as amended. For ease of reference, certain terms used in this Code of Practice are defined in Section 1.

Cyber security

3.1 What is cyber security?

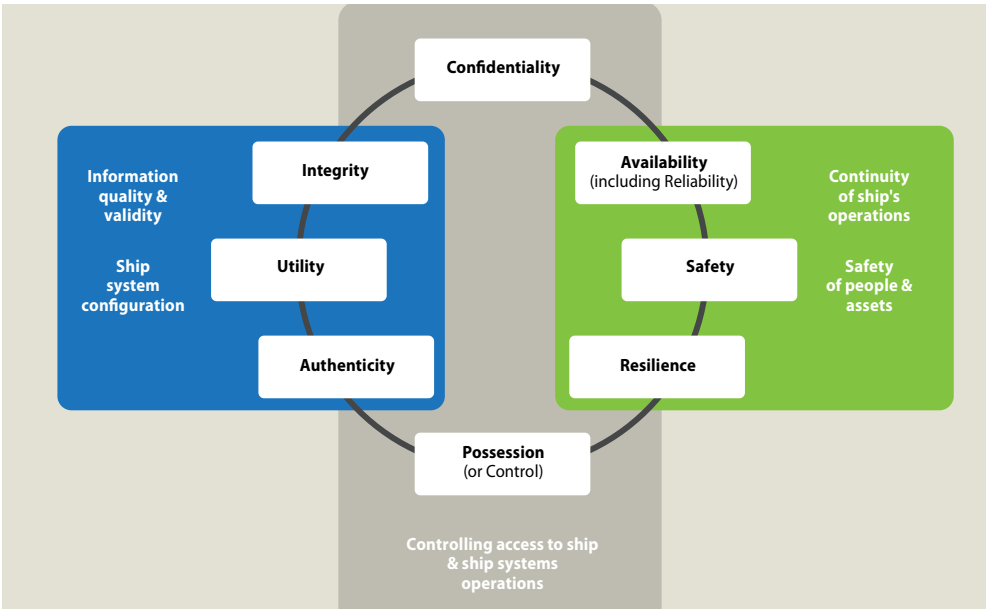
Cyber security can be defined as 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets'[1].

Within this definition, 'cyber environment' comprises the interconnected networks of both IT and cyber-physical systems utilising electronic, computer-based and wireless systems, including the information, services, social and business functions that exist only in cyberspace. On a ship the computer-based systems will comprise a range of information technology components (for example, personal computers (PCs), laptops, tablet devices, servers and networking component such as routers and switches, etc.) and operational technology (for example, control systems, sensors, actuators, radar, etc.). Further details of the groups or classes of systems found on a ship are provided in Appendix A.

The 'organization and user's assets' includes connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted, processed and/or stored data and information in the cyber environment.

Cyber security strives to attain and maintain eight general security objectives, shown in Figure 3.1 and described in Appendix A:

▼ **Figure 3.1** Cyber security attributes[2]



1 International Telecommunications Union, "Overview of cyber security", ITU-T X.1205, 2008, Geneva, Switzerland

2 Adapted from Figure 2 of Boyes, H. (2015) "Cybersecurity and Cyber-Resilient Supply Chains". Technology Innovation Management Review, 5(4): 28-34

The varied nature of cyber security threats means that there is no single approach that is capable of addressing all the resultant risks. The rate of change of technology and the steady flow of serious vulnerabilities in operating systems, software libraries and applications, means that any strategy needs to be kept under regular review.

Business change also has a significant impact on cyber security, for example, the introduction of bring-your-own-device (BYOD) and the trend to deliver some assets as services, for example, the provision of power plants/turbines remotely managed by a third party that offers power/propulsion as a service.

Within the maritime environment a variety of IT-based devices may legitimately be brought onto the ship, for example devices owned by the shipboard personnel or shore-based contractors. The nature of these devices and their relative cyber hygiene could have a significant impact on the cyber security of the ship, particularly if they are connected to sensitive communications or network infrastructure within the ship or critical ship systems.

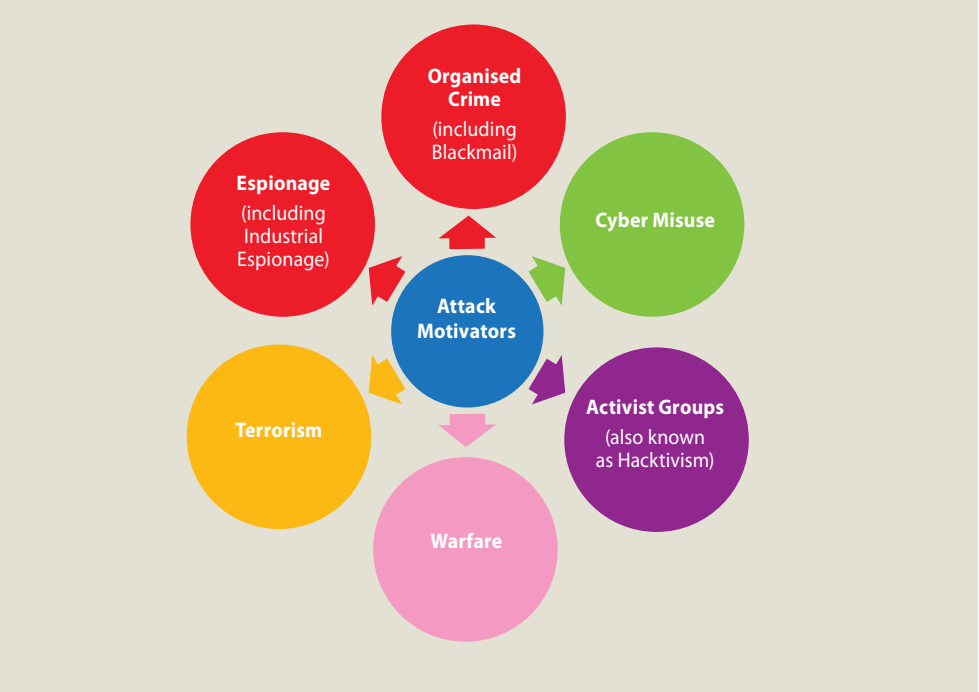
3.2 What are the threats that cyber security is seeking to address?

The motivation for a cyber-attack on a ship system, as illustrated in Figure 3.2, may be for one of the following six purposes.

(a) cyber misuse – this includes low-level criminal activities including vandalism and disruption of systems, defacement of web sites and unauthorised access to systems. The acts may be perpetrated by script kiddies[3] or through insider activity by disgruntled personnel and contractors. Where researchers access a system without authority from the system's owner, their actions may not be malicious but are nevertheless deemed a criminal act by the UK Computer Misuse Act.
(b) activist groups (also known as 'hacktivism') – seeking publicity or creating pressure on behalf of a specific objective or cause, for example, to prevent the handling of specific cargoes or to disrupt the operation of the ship. The target may be the ship itself, the operator of a ship or a third party such as the supplier or recipient of the cargo.
(c) espionage – seeking unauthorised access to sensitive information (intellectual property, commercial information, corporate strategies, personal data, pattern of life) and disruption for state or commercial purposes.
(d) organised crime – largely driven by financial gain, this may include criminal damage, theft of cargo, smuggling of goods and people, and seeking to evade taxes and excise duties.
(e) terrorism – use of the ship to instil fear and cause physical and economic disruption.
(f) warfare – conflict between nation states, where the aim is disruption of transhipsystems/infrastructure to deny operational use or disable specific ships, such as product tankers.

3 Script Kiddies generally refers to an unskilled individual who utilises scripts or programs written by others to attack systems.

▼ **Figure 3.2** Motivation of cyber security threat actors



The threat actors may be classified into one of seven categories, these are detailed further in Appendix A:

(a) individuals, for example, 'script kiddies' and insiders;
(b) activist groups, also known as 'hacktivists';
(c) commercial competitors;
(d) cyber criminals;
(e) terrorists; and
(f) nation states and state sponsored actors.

Any of these threat actors are equally relevant to: elements of the ship's systems located remotely; ship information/data stored on external servers; services delivered by third parties; and the ship's supply chain.

When considering the potential threats from the hostile groups listed above, it is important to recognise that there may be some convergence between the aims and objectives of individual groups. For example, some of the malware developed by cyber-criminal gangs includes sophisticated command and control functionality, allowing secure exfiltration of information and update of modular components to deliver new or varied exploits over time. Thus a machine or device that was compromised initially for financial crime could be used in future to access sensitive data or to provide a backdoor to allow attacks on the ships themselves.

3.3 What are the effects that threat actors are trying to achieve?

Whatever the aim and motivation for attacking a ship or fleet of ships, the threat actors will have an outcome that they are attempting to achieve. These effects may be aimed at the overall business, the ship or the ship subsystems and are grouped into the following categories:

(a) destroy – examples may include the destruction of cargo, ship, or port such that they are no longer available for use.
(b) degrade – examples may include impacting the speed or manoeuvrability of the ship, the ability to navigate accurately or monitor the local environment accurately to the point where the ability of the ship to operate is significantly impaired.
(c) deny – examples may include the denial of access to ship systems or information/data possibly for such reasons as extortion for financial gain or to mount a physical attack on the ship for kidnap and ransom purposes.
(d) delay – examples may include to delay the timely operation of the ship or ship subsystems such that the knock-on effect may impact business operations or cause penalties to be incurred.
(e) deter – examples may include influencing the business from operating in certain areas of the world oceans, operating in specific markets or accessing specific ports from a commercial perspective.
(f) detect – examples may include the detection of people, cargo or ship locations and to track such that planned physical theft or cargo manipulation might take place.
(g) distract – examples include the ability to alter the state of a sensor so to provide a distraction whilst a data/information extraction takes place.

The examples given are not exhaustive and appropriate effects are selected when considering the threat actor and the motivation behind any attack.

3.4 Resilience of ship systems and infrastructure

Resilience of ship systems is closely linked to safety and the higher the potential safety risk so the higher level of redundancy and availability of critical systems. These systems are monitored such as to provide constant situational awareness based on sensor data received from a number of sensor types.

The integrity and availability of such data is therefore critical for the safe and secure operation of the ship and its systems especially where systems are integrated into a system of systems each interdependent on the others for data acquisition, computational analysis or physical actuation.

Understanding these interdependencies and relationships between systems at a data or information level is essential in maintaining the integrity of the overall system of systems.

In addition to the human threat actors, there are resilience threats to ship systems arising from natural causes, including: solar events; weather; flora and fauna. Their effects may result in damage, failure or significant impairment to ship systems, which may result in the loss or corruption of ship data, and subsequent loss of integrity or availability of the subsystem.

An example of the impact of natural causes on ship systems is a terrestrial or solar storm causing interference with communication systems and the loss of ship-to-shore link.

In addition the reaction to false sensor data due to malfunction also needs to be considered. The absence of data may be as significant as a constant stream of data when considering the resilience of the various systems.

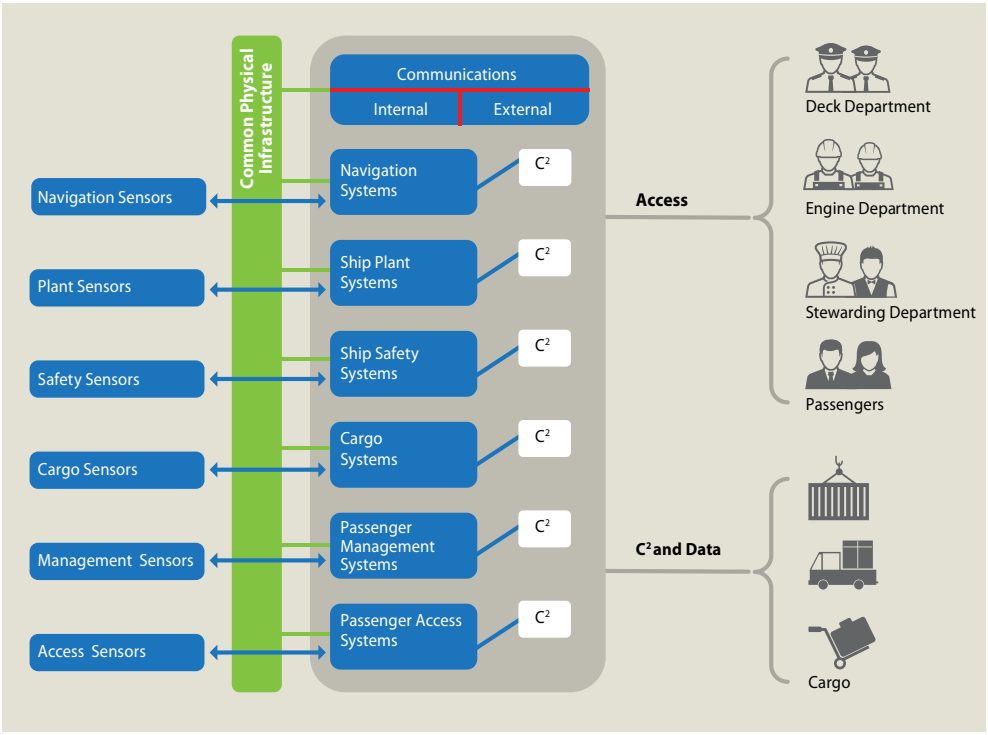
SECTION 4

Cyber security of ships

4.1 Why is cyber security important to ships?

A ship is a complex cyber-physical engineered system that encompasses both waterborne activities and systems, and remote elements such as navigation signals. As illustrated in Figure 4.1, and examined in more detail in Appendix A, a ship comprises five main asset types (i.e. plant and machinery, operational technology, information technology, radio frequency (RF) communications, and navigation systems) that are used to provide a range of operational services and where technology plays an increasingly important role.

▼ **Figure 4.1** Ship assets affected by cyber security



The loss, or compromise, of one or more of these assets has the potential to impact upon:

(a) the health and safety of staff and other people impacted upon by the work activities being undertaken and to whom a duty of care is owed;
(b) the ability of the ship to operate safely and to not endanger other ships, maritime structures or the environment; and
(c) the speed and efficiency at which the ship can operate.

Further, the failure of a Company or shipboard personnel to appreciate the structure and operation of its assets, systems and associated business processes may result in a number of undesirable situations, including:

(a) accidental or inadvertent exposure of sensitive systems, applications or data to unauthorised users;
(b) loss of resilience or system redundancy; and
(c) emergent failure modes that result in the cascade or catastrophic failure of critical systems or processes.

Any of the types of failure described can also have significant economic and reputation consequences.

4.2 Cyber security standards, guidance and good practice

There is a wide range of security-related standards and best practice guidance available that apply to IT and industrial control systems. The bibliography in Appendix H lists a broad range of such documents. Much of the material is written from an information systems security perspective and needs to be carefully interpreted when applying it to systems in the maritime environment. For example, the application of some security techniques to safety critical systems may hinder their operation in an emergency situation.

A complexity increasingly occurring in the maritime environment is the integration of safety critical alarm and/or control systems with conventional enterprise and office IT systems. This integration requires careful management by the Company as the office elements may operate under security policies and procedures originating from ISO 27000 series documents, whereas control and safety systems are more likely to operate under regimes determined by the IEC 61508 and IEC 62443 standards.

Note: The UK Government has produced two sets of guidance that are generally applicable to organisations, the 10 Steps to Cyber Security and the Cyber Essentials scheme. The latter addresses basic technical control that all organisations should have in place to mitigate common cyber security issues.

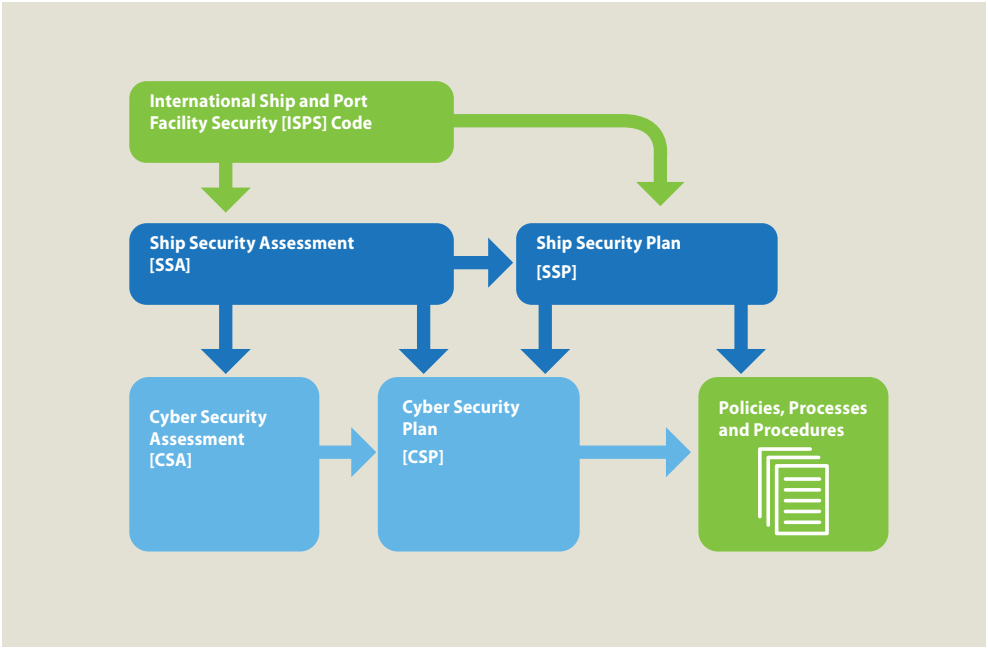
SECTION 5

Developing a cyber security assessment (CSA)

The relationship of the CSA to the ship security assessment (SSA) and ship security plan (SSP) that are required by the UK and European legislation and the ISPS Code is illustrated in Figure 5.1.

Note: In Part B of the ISPS Code, paragraphs 8.1 to 8.10 provide guidance on aspects to be included in the SSA, these include: radio and telecommunication systems (including computer systems and networks), and other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility. Assessing the cyber security of ship assets requires specialist knowledge and expertise and as such it is recommended that suitably qualified and experienced individuals undertake the preparation of the CSA and CSP. Given the rapidly changing nature of the cyber security landscape there is a need to review both documents more frequently than the quinquennial review required for the SSA and SSP.

▼ **Figure 5.1** Relationship of the CSA and CSP to other documents



The purpose of performing the cyber security assessment is to adopt a risk management approach to assessing and mitigating the risks associated with the threat actors that are relevant to the ship or ships that are being assessed. The benefits of adopting this approach are that cyber security risks may be prioritised, enabling appropriate and proportionate investment to be made in a portfolio of security controls to mitigate those risks with potentially the greatest impact.

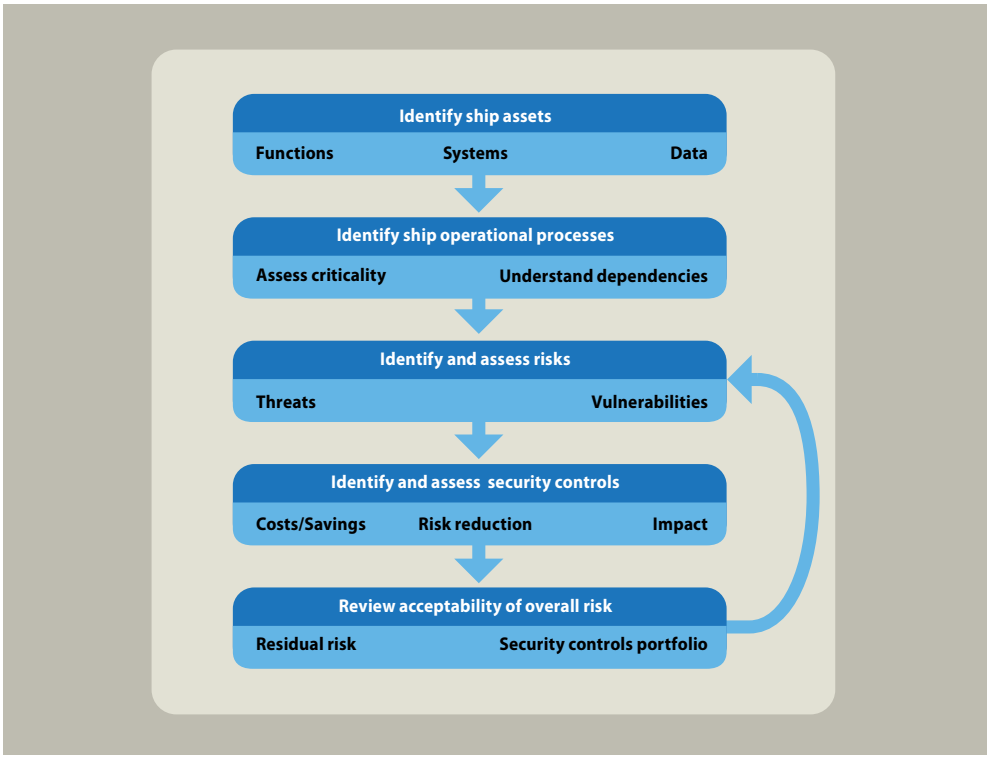
Ship security assessments are conducted in compliance with the ship security standards. The purpose of these assessments is principally to identify vulnerabilities in physical and personnel security measures and the Company's/ship's business processes that may

lead to a security incident. It is intended that wherever appropriate the CSA should build upon the existing security assessments.

As set out in the ship security standards and illustrated in Figure 5.2, these assessments should encompass the ship as a complete cyber physical engineered system and will involve:

(a) identification and evaluation of essential or sensitive assets and infrastructure (for example, facilities, systems and data) considered important to protect, and the external infrastructure systems upon which they depend;
(b) identification of the ship's business processes using the assets and infrastructure, so as to assess criticality of assets and understand any internal and external dependencies;
(c) identification and assessment of risks arising from possible threats to the assets and infrastructure, vulnerabilities and the likelihood of their occurrence, in order to establish the need for and to prioritise security measures;
(d) identification, assessment, selection and prioritisation of security controls and procedural changes, based on their costs, the level of effectiveness in reducing the risk and any impact on the ship's operations; and
(e) identification of the acceptability of the overall residual risk, including human factors, and weaknesses in the infrastructure, policies and procedures, based on the portfolio of security controls that have been selected.

▼ **Figure 5.2** Overview of CSA process



Where these assessments do not cover the full range of potential cyber security threats, the Company/ship should produce a CSA that includes each of the aspects listed in this section.

For further details of a process to create a CSA see Appendix B. This appendix addresses the assessment of cyber security risks, the identification and prioritisation of risk treatments (security controls) so as to provide a basis for the cyber security plan (CSP).

SECTION 6

Developing a cyber security plan (CSP)

The ship security assessments form the basis of the security plans for the ship. These plans should address the predominantly physical and personnel issues identified in the relevant assessment through the establishment of appropriate security measures designed to minimise the likelihood of a breach of security and the consequences of potential risks. It is intended that wherever appropriate the CSP will build upon the existing ship security plan (SSP) and may be an annex to it. Thus the measures aimed at reducing the risk of unauthorised access to the ship should also give a degree of protection to its cyber-physical systems.

A CSP should perform the same function for the issues identified in the CSA, also taking into consideration the impact of measures set out in the security plan for the ship and its systems. Its relationship to other key documents is illustrated in Figure 5.1. The recommended contents of a CSP are set out in Appendix C.

When developing the CSP it is essential that a holistic approach be adopted, covering the people, process, physical and technological aspects of the ship. From a cyber security perspective, the CSP should contain or reference:

(a) the policies that set out the security-related business rules derived from the SSP;
(b) the processes that are derived from the security policies and provide guidance on their consistent implementation throughout the lifecycle and use of the ship assets; and
(c) the procedures that comprise the detailed work instructions relating to repeatable and consistent mechanisms for the implementation and operational delivery of the processes.

With a large proportion of security breaches caused by people and poor processes, it is essential that personnel, process and physical aspects directly related to the technological systems for which cyber security measures are required, are also considered and appropriate measures put in place. For example, sensitive ship systems may be protected from unauthorised access or modification as follows:

(a) physical – the system and its components may be located in a restricted access area, to which only those personnel who have been authorised for access are permitted unsupervised access, a log of all authorised personnel is kept and regularly updated;
(b) personnel – personnel with privileged (administrative, engineering or technical support) access to the systems are subject to pre-employment screening and periodic background checks;
(c) process – processes are in place to ensure that all access to the systems is monitored and logged, and that personnel accessing controlled spaces or sensitive system, who were not subjected to the screening and background checks (see also Appendix G), are supervised by a person who is authorised to access the systems;
(d) technical – measures are in place to check any removable media or portable devices that will be connected to the system for malware (for example, software updates on USB memory sticks or diagnostic software on laptops or tablet devices). Access to systems consoles, displays, etc is password protected.

The measures required in each of the aspects will also depend on the level of resilience that the ship may call upon. Appendix D provides guidance on how to develop appropriate mitigation measures, which should inform the development of the CSP and the supporting policies, processes and procedures.

Regular training and assessment should be established for all those who are granted 'authorised' status for access to systems and subsystems to ensure that appropriate cyber hygiene is carried out when accessing systems for whatever reason.

The completed CSP for the ship should be protected from unauthorised access or disclosure and should form an annex of the SSP.

6.1 Review of the CSP

The CSP should include a suitable mechanism for performing periodic, at least annual, reviews of the CSP to verify that it remains fit for purpose. Where necessary, the CSP should be updated to reflect any identified gaps, shortcomings or organizational changes, or changes which have arisen for political, economic, social, technological, legal or environmental reasons, and which impact on the ship or ship assets.

Note: Whilst the ISPS Code only requires the SSP to be required every 5 years, given the rapidly evolution of cyber security threats it is good practice to review the CSP more frequently.

The CSP should establish a suitable mechanism for performing ad-hoc risk reviews to identify and assess the impact of any changes on ship assets and to update the CSA as described in Section B.6.

6.2 Monitoring and auditing of the CSP

The CSP should set out the appropriate and proportionate monitoring and auditing measures that will take place across the lifecycle of all ship assets, and are aligned where applicable with the business risk strategy. This monitoring or auditing will be in addition to any actions that may result from an incident or breach. The CSP should require that only those suitably qualified and experienced would undertake this monitoring and auditing work.

Note: Paragraph 9.4.1 of Part A of the ISPS Code states that "Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship." This is good practice and should be adhered to wherever practicable.

Measures should include assessing:

(a) the implementation of all security policies, processes and procedures affecting the ship assets, including the handling or storage arrangements implemented for security-sensitive and sensitive information;
(b) the compliance of its supply chain with the security policies, processes and procedures specified in the CSP, as a minimum on a risk-based sampling approach; and
(c) the management of security controls that operate throughout the operational lifecycle of the ship assets.

Monitoring should continue through an event that causes the failure or interruption of one or more systems. An extreme weather event or other such occurrence does not remove the need for effective security and how the systems perform will inform subsequent development and loss exposure.

Whilst the Company may delegate some responsibility for compliance verification to a supplier, it should retain accountability for the overall effectiveness of security controls.

Managing cyber security

Having established the cyber security management framework through the creation of the CSA and CSP, it is important that appropriate management and operational arrangements are in place, including:

(a) the identification of the individual or individuals responsible for the cyber security of the ship. Individuals fulfilling these roles being designated as a cyber security officer (CySO);
(b) the establishment of a security operations centre (SOC), (see Section 7.2 for more information);
(c) the arrangements for providing information to third parties; and
(d) the arrangements for managing security incidents or breaches.

7.1 Role of the CySO

Depending on the size or nature of the ship and/or fleet, the CySO role may be located on board the ship, for example a cruise liner sailing on the high seas, or shore-based for ships that routinely operate either solely in British waters or working predefined routes between specific ports, or where a suitable resource is not available on board. The CySO is responsible for all security aspects of cyber-enabled systems on the ship, i.e. both the IT, OT and communications systems.

The CySO should also be responsible for:

(a) liaising with the Company security officer (CSO) on aspects relating to physical, personnel and process security; and
(b) ensuring the development, periodic review and maintenance of the CSA/CSP; and
(c) implementing and exercising the CSP.

Where the CySO has insufficient knowledge of all cyber security issues and solutions, they should seek specialist cyber security advice from an appropriate professional source.

Note: The professional source may be provided by the Company or provided as a professional support contract arranged by the Company.

The CySO should maintain awareness of legal and regulatory changes that could affect the cyber security of ship assets and where necessary, make adjustments in policies, processes and procedures to comply with those changes.

Note: The awareness of legal and regulatory changes may be monitored by the Company, or provided through a professional support contract arranged by the Company, and delivered to the CySO as a periodic update.

For the CSP and associated security policies, processes and procedures to be effective, it is essential that there is a flow down of responsibility within both the Company and the contracts/supply chain. Responsibility for cyber security may be shared by the CySO with other managers and service providers, although accountability should remain with the CySO, who is of sufficient seniority and has the authority to act.

The CSP should detail the:

(a) maintenance of security accountability within the Company's organisation; and
(b) management of security responsibilities within the supply chain, including the requirement for security to be retained at senior levels within the supply chain, with responsibility delegated appropriately, in order that it may be effectively and efficiently managed.

Where the Company makes extensive use of contract personnel, the CSO should ensure appropriate measures are used for the secure procurement of contracting personnel, which includes appropriate screening or background checks. These checks should also be in place for staff employed through other mechanisms.

Where the ship operates both within British waters and in foreign waters, including the high seas, the CySO should understand the jurisdiction issues regarding law enforcement and cyber security incidents. The principles set out in Table 7.1 are likely to apply, however the issue of jurisdiction is a complex area for cyber security and maritime offences and expert legal advice should be sought in the event of an incident.

▼ **Table 7.1** UK court jurisdiction over cyber security incidents on ships

Cyber security incident alleged to have been caused by	Jurisdiction
A British Subject: **(a)** on a British ship, in either British or foreign waters, including high seas; **(b)** belonging to a British ship, in either British waters or high seas; or **(c)** on a foreign ship, in either British or foreign waters, including high seas.	Full jurisdiction of UK Courts (Magistrates' Courts Act 1980, s.3A, Senior Courts Act 1981, s46A(1) and Merchant Shipping Act 1995, s280 – 282)
A British Subject, belonging to a foreign ship, in a foreign port/harbour.	No jurisdiction (See Note)
A person who is not a British Subject, on a British ship, in British waters or high seas.	Full jurisdiction of UK Courts (Magistrates' Courts Act 1980, s.3A, Senior Courts Act 1981, s46A(1) and Merchant Shipping Act 1995, s280 – 282
A person who is not a British Subject, on a foreign ship, in British waters (12 mile limit)	Full jurisdiction of UK Courts (Territorial Waters Jurisdiction Act 1878, s2 & Territorial Sea Act 1987, s1)
A person who is not a British Subject, on a foreign ship, outside British waters, i.e. foreign waters or high seas.	No jurisdiction

Note: The Computer Misuse Act 1990 potentially applies to actions by a British Subject, irrespective of their location or the vessel, although application of the Act would be difficult without the co-operation of the foreign ship and/or jurisdiction.

Where a UK court has jurisdiction, the procedures for handling a serious cyber security incident should include seeking advice/assistance from the UK Authorities (NCSC, DfT and UK law enforcement).

For some ships the provisions of the directive on security of network and information systems (the upcoming NIS Directive)[1] may apply to cyber security incidents affecting the ship.

7.2 Security operations centre (SOC)

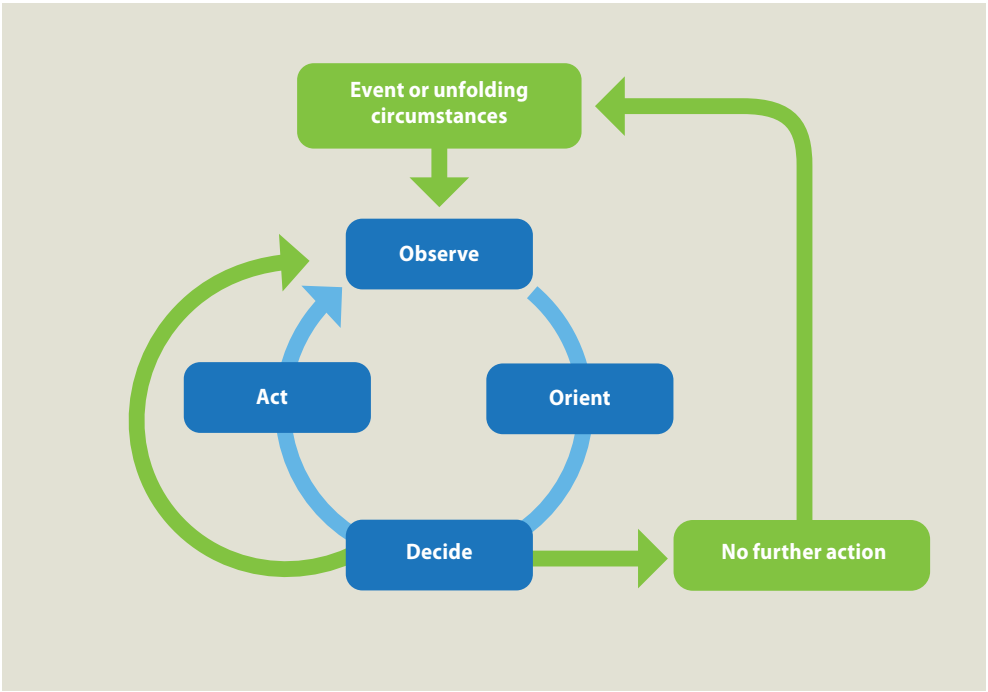
A SOC acts as a centralised unit dealing with security issues affecting the cyber-physical systems on or connected to a ship or fleet of ships, including those relating to cyber security. It may form part of a Company's operations centre supervising the operation of a number of ships, including the management of business continuity and disaster recovery activities.

Note: The nature or scale of any SOC will depend on the size and nature of the ship and/or fleet. Where the Company has an existing operations centre the SOC may form part of that centre and should address security in a holistic fashion, i.e. encompassing personnel, physical and cyber security.

The key functions of a SOC as illustrated in Figure 7.1, are to:

(a) observe, by maintaining situational awareness, i.e. understand potential, emerging and actual threats to the ship's operations. Observation includes detection of unauthorised changes to ship systems or ship data, unsecure modes of operation and unauthorised access to ship assets.
(b) orient, by analysing the risk to operations from new or changed threats and determine whether proactive measures are required to reduce the risk to an acceptable level.
(c) decide what action may be appropriate either to deny further access to the ship asset or to respond to the event by identifying suitable security controls.
(d) act, by implementing the decision(s).

▼ **Figure 7.1** Key functions of a SOC

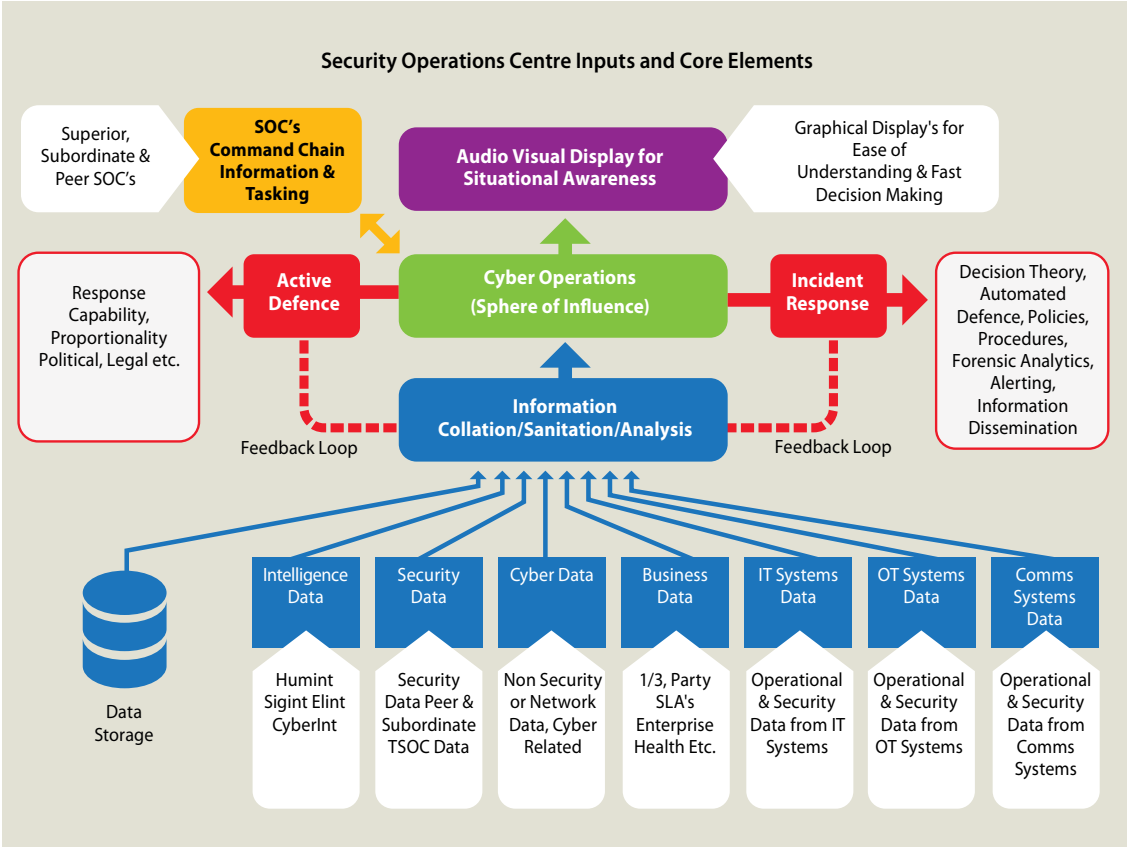


1 See Directive (EU) 2016/1148 http://data.europa.eu/eli/dir/2016/1148/oj, which comes into effect in 2018

In observing the operating environment SOC personnel should maintain situational awareness of the general threat environment. From a cyber security perspective, this may involve accessing threat intelligence information from both public and private sector sources. The benefits of belonging to a threat intelligence sharing scheme like the UK CiSP[2] include:

(a) engagement with industry and government counterparts in a secure environment;
(b) early warning of cyber threats;
(c) ability to learn from experiences, mistakes, successes of other users and seek advice;
(d) an improved ability to protect their corporate and operational networks; and
(e) access to free network monitoring reports tailored to your organisation's requirements.

▼ **Figure 7.2** General schematic of a SOC



7.3 Provision of information to third parties

The Company and ship's master need to take appropriate measures to reduce the risk of sensitive information being released publicly or provided to unauthorised third parties. This can occur through public presentations, conference papers, marketing and publicity material, or by the use of social media both by their organisation and their staff, contractors and supply chain. The implementation of an appropriate data loss prevention solution should also be considered. For further information see Appendix E.

2 In the UK, NCSC operates a joint industry and government Cyber-security Information Sharing Partnership (CiSP) to share cyber threat and vulnerability information. https://www.ncsc.gov.uk/cisp

7.4 Handling security breaches and incidents

The CSP should detail the arrangements for handling security breaches and incidents, whether they occur accidently or deliberately. The ISPS Code recognises that incidents generally fall into two categories:

(a) those considered to be sufficiently serious that they should be reported to the relevant authorities by the CSO, for example:

- **i** unauthorised access to, misuse or fraudulent use of sensitive ship systems;
- **ii** unauthorised changes to or loss of information from sensitive ship systems;
- **iii** attempted or successful cyber-attacks on ship systems affecting the safety of life, the ship or its cargo;
- **iv** damage to the ship, where it is suspected or evident that a cyber security breach or breaches are a contributory factor;
- **v** attempts to manipulate cargo manifests to facilitate the smuggling, illegal or unauthorised carriage of prohibited or controlled goods or materials (for example, illegal drugs, weapons, explosives, items whose carriage is restricted by international treaty, etc.); and
- **vi** attempts to affect passengers, for example fraud associated with theft or unauthorised access to personal data or personally identifiable information or compromise of ship systems processing bank or credit card information.

(b) those of a less serious nature, but which require reporting to, and investigation by, the SSO and for cyber incidents the CySO, for example:

- **i** cyber security incidents affecting the ship and/or its cargo that are not covered by the examples in point (a) (i) above; and
- **ii** malware incidents affecting non-sensitive systems including the personal devices owned by the crew.

A cyber security incident is likely to arise from unauthorised access to, misuse or fraudulent use of, ship systems or related assets and may result in:

(a) loss or theft of assets, including documents and storage media;
(b) unauthorised access to data or information
(c) loss, compromise, unauthorised manipulation or change of data or information;
(d) loss or compromise of ship assets connected to its systems;
(e) planting of bugs or other surveillance devices; and
(f) insertion of malicious software.

For further information see Appendix F.

Note: In the UK the NCSC operates a cyber security incident reporting service for victims of a significant cyber security incident[3], this replaces the service formerly operated by CERT-UK. CiSP members should consider submitting an incident report on the CiSP platform as a means of sharing timely threat information with other members. Depending on the nature of the incident it may be appropriate to report it to Action Fraud or relevant national equivalent.

3 See https://www.ncsc.gov.uk/articles/get-help-significant-cyber-incident-guidance

APPENDIX A

Understanding cyber security

A.1 Cyber security attributes

The maritime environment involves a variety of technologies, existing and emerging, and the cyber security approach adopted will vary from ship to ship, depending on the complexity, ownership, use and the supply chain supporting the design, construction operation and occupation of the ship. Cyber security is therefore best addressed by considering a set of security attributes, thus allowing appropriate solutions to be adopted, based on the nature of the cyber-physical system (i.e. the ship, high-speed craft or MODU) and potential threats.

The key attributes of cyber security as applied to cyber-physical systems are outlined below. When considering these attributes, a risk management approach should be adopted, which will inform the degree to which any preventative or protective measures are implemented and the degree to which any residual risk is acceptable.

(a) Confidentiality – the control of access and prevention of unauthorised access to ship data, which might be sensitive in isolation or in aggregate. The ship systems and associated processes should be designed, implemented, operated and maintained so as to prevent unauthorised access to, for example, sensitive financial, security, commercial or personal data. All personal data should be handled in accordance with the Data Protection Act and additional measures may be required to protect privacy due to the aggregation of data, information or metadata.

(b) Possession and/or control – the design, implementation, operation and maintenance of ship systems and associated processes so as to prevent unauthorised control, manipulation or interference. The ship systems and associated processes should be designed, implemented, operated and maintained so as to prevent unauthorised control, manipulation or interference. An example would be the loss of an encrypted storage device – there is no loss of confidentiality as the information is inaccessible without the encryption key, but the owner or user is deprived of its contents.

(c) Integrity – maintaining the consistency, coherence and configuration of information and systems, and preventing unauthorised changes to them. The ship systems and associated processes should be designed, implemented, operated and maintained so as to prevent unauthorised changes being made to assets, processes, system state or the configuration of the system itself. A loss of system integrity could occur through physical changes to a system, such as the unauthorised connection of a Wi-Fi access point to a secure network, or through a fault such as the corruption of a database or file due to media storage errors.

(d) Authenticity – ensuring that inputs to, and outputs from, ship systems, the state of the systems and any associated processes and ship data, are genuine and have not been tampered with or modified. It should also be possible to verify the authenticity of components, software and data within the systems and any associated processes. Authenticity issues could relate to data such as a forged security certificate or to hardware such as a cloned device.

(e) Availability (including reliability) – ensuring that the asset information, systems, and associated processes are consistently accessible and usable in an appropriate and timely fashion. To achieve the required availability may require each of these to have an appropriate and proportionate level of resilience. A loss of availability could occur through the failure of a system component, such as a disk crash, or from a malicious act such as a denial of service attack that prevents the use of a system connected to the Internet.

(f) Utility – that asset information and systems remain usable and useful across the lifecycle of the ship asset. The ship systems and associated processes should be designed, implemented, operated and maintained so that the use of ship assets is maintained throughout their lifecycle. An example of loss of utility would be a situation where a ship system has been changed or upgraded and the file format of historic data is no longer intelligible to the system. There has been no loss of availability but the data is unusable.

(g) Safety – the design, implementation, operation and maintenance of ship systems and related processes so as to prevent the creation of harmful states which may lead to injury or loss of life, or unintentional physical or environmental damage. A safety issue could arise through malware causing a failure to display or communicate ship systems alarm states. For example, the failure of a motion or proximity detector or other sensors could result in damage to property or loss of life.

(h) Resilience – the ability of the asset information and systems to transform, renew and recover in a timely way in response to adverse events. The design, implementation, operation and maintenance of ship systems and associated processes should be such that cascade failures are avoided. In the event that either a system or associated process suffers disruption, impairment or an outage occurs, it should be possible to recover a normal operating state, or acceptable business continuity state, in a timely manner.

A.2 Threat actor groups

A.2.1 An individual

The severity and sophistication of the threat will be determined by the individual's capabilities, for example:

(a) a negligent, careless or ignorant employee or contractor fails to follow acceptable use or other security policies, or through error or omission, compromise system security.

(b) non-malicious individuals who are not seeking to harm systems or data, but may access the systems without the permission or knowledge of the owner and may cause accidental damage. The motivation of such agents is generally to investigate weaknesses and vulnerabilities in systems.

(c) a disaffected employee or contractor with limited IT skills – motivations will vary; the intent may be to steal or leak sensitive information, to sabotage or disrupt ship operations, etc. The amount of damage they can inflict will depend on their role, system access rights and the efficacy of cyber security measures related to the ship systems and data.

(d) a disaffected employee or contractor with significant IT skills, including system administrators – these individuals can do significant damage, particularly if they have wide ranging systems access with administrative privileges. They may have sufficient knowledge and ability to bypass controls and protective measures, and may be adept at removing evidence of their activities, for example, deleting or modifying entries in system logs. For sensitive roles there is a need to consider

aftercare of disaffected individuals leaving the organisation, based on an assessment of risk and monitoring of social media feeds.

(e) script kiddies – individual hackers with limited knowledge who use techniques and tools devised and developed by other people. The ready availability of hacking and denial of service tools on the internet (in some cases distributed with technical magazines) means that the level of technical understanding required to launch an attack has been significantly reduced.

(f) cyber vandals – this group can be very knowledgeable and may develop or further expand their own tools. Their motives are neither financial nor ideological – they carry out hacks or develop malware because they can and want to show what they can do. They may, for example, deface a website or break into a server to steal user credentials, which are then posted on a public website to demonstrate their ability.

(g) lone wolf – individuals outside of the organisation possessing advanced technical knowledge. This group may be adept at removing evidence of their activities, for example deleting or modified entries in system logs. They may also have sufficient knowledge and ability to bypass controls and protective measures. The number of such individuals is currently small, but may expand as a result of increased awareness of technical systems amongst the general population, or as members of nation state groups leave government service.

A.2.2 Activist groups

Often referred to as hacktivists, these groups comprise ideologically motivated individuals that may form dynamic groups or sub-groups. Their actions are effectively online protests, which may have the aim of disrupting systems or acquiring confidential or sensitive information for publication or dissemination so as to embarrass their target(s). The impact of small activist groups can be significantly magnified when, as some groups have demonstrated, they recruit or persuade naïve third parties to join in by allowing the installation of malicious software on the recruits' computers, thus creating botnets[1] and magnifying the effect of any distributed denial of service (DDoS) attacks.

A.2.3 Competitors

This group is typically large corporations seeking to create competitive advantage. They may act directly or through third parties, with the aim of harming a rival by collecting business intelligence, stealing intellectual property, gathering competitive intelligence on bids or disrupting operations to cause financial or reputational loss. Depending on size, sector, geographic location and the sophistication of a large corporation's cyber capabilities they may be able to perform sophisticated malicious activities to target and infiltrate their competitors.

A.2.4 Cyber criminals

These are sophisticated criminal groups perpetrating a wide range of illegal IT-enabled crime. The motivation is to profit from illegal activities, and their focus has mainly been on fraud, thefts from accounts and theft of intellectual property. However, cyber-criminal activities also include blackmail and extortion through use of malware to encrypt data or threats of denial of service attacks on corporate websites. In respect of ports, cyber criminals may seek to intercept or access information related to cargo shipments or to

---

1 A botnet is a network of computers infected with malicious software (malware) and controlled as a group without the users' and/or owners' knowledge, they may be used to send spam or in DDoS attacks.

security arrangements as a precursor to criminal activities or a physical attack on these premises. The sophistication of the malware used by these groups is increasing and there is evidence of a cyber-crime market, where developers, providers and operators create, supply and operate sophisticated malware and cyber-crime tools on a commercial basis, making their tools available to third parties.

A.2.5 Terrorists

Terrorists are becoming increasingly IT aware, and already make extensive use of the Internet to distribute propaganda and for communications purposes. Well-funded groups could take advantage of the service offered by cyber criminals, seek support from a nation state or encourage internal members to adopt these methods of attack. With the widespread use of electronic and computer-based technologies in the maritime environment, terrorist groups could rely on the various toolkits available for download to disrupt or damage ships by attacking ship and/or connected shore-based systems. Terrorists may also exploit poorly secured ship data to enable remote hostile reconnaissance of targets, thus reducing the time they need to spend in or near their target.

A.2.6 Nation states and state sponsored threat actors

It is acknowledged that some nation states are actively involved in cyber-attacks on a wide range of organisations to acquire state secrets or sensitive commercial information and intellectual property. They may also threaten the availability of critical infrastructure in other nation states. During periods of heighted international tension and conflict, these activities may include more widespread attacks as evidenced by malware such as Stuxnet[2], Duqu[3] and Flame[4].

The state sponsored threat actors effectively have the capacity and sophisticated technical support available to a nation state made available by the sponsoring nation. This group could include cyber fighters, i.e. groups of nationally motivated individuals who threaten or attack other groups, businesses and the infrastructure of other nation states. The cyber fighters may be seen as a type of hacktivist, but their interest is the support of a nation state and as such they may enjoy significant sophisticated technical support from that nation state.

A.3 Ship assets and cyber security

The complexities of systems on board ships are generally related to size and operation. A ship requires systems to provide and control propulsion, steering, ballast, etc. however as soon as you add passengers you add to the quantity and complexity as systems are added to provide facilities and to manage the human cargo.

The ship by its very nature has to work untethered from land and the only connection provided when at sea is via one of many possible communications channels providing both voice and data exchange. The vessel may therefore from a cyber perspective be considered as a 'system of systems' operated in a contained environment.

---

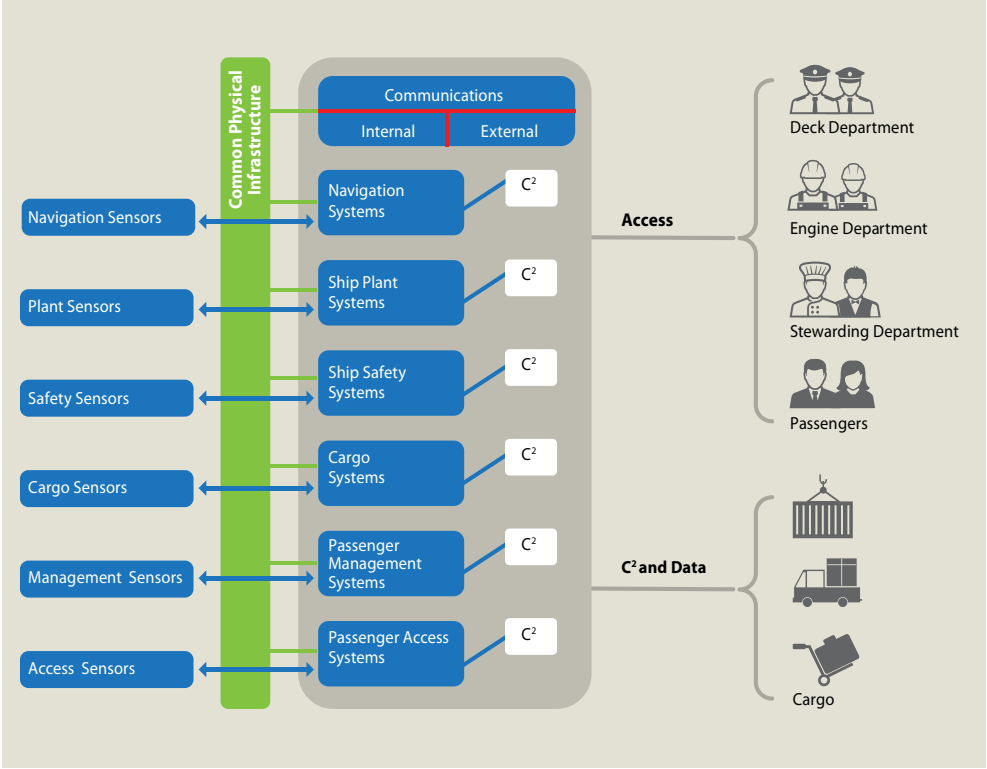
2 For further information see – http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

3 For further information see – http://resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen/

4 For further information see – http://www.wired.com/2012/05/flame/

The number of class societies[5] worldwide, the diversity of ship designs and the number of subsystem manufacturers presents significant complexity when developing a cyber model that is representative and capable of being used for all classes of ship.

▼ **Figure A.1** Simplified ship systems diagram



For the purposes of developing appropriate and proportionate cyber security measures, each of the technical systems in place may be considered as largely located in, or directly related to one of the following categories:

(a) communications – systems provided for internal, ship-to-shore and ship-to-ship communications. These may include remote monitoring systems such as voyage data recorders and systems that monitor the performance of the vessels subsystems. Such systems often connect to OT and navigation systems before the data is communicated often via satellite.
(b) navigation systems – systems that are either directly for, or provided in support of ship navigation.
(c) plant systems – systems used for monitoring and control of any machinery and plant associated with the general operation of the vessel, not covered in other categories.

---

5 Classification societies set technical rules based on experience and research, confirm that designs and calculations meet these rules, survey ships and structures during the process of construction and commissioning, and periodically survey vessels to ensure that they continue to meet the rules. Classification societies are also responsible for classing oil platforms, other offshore structures, and submarines. This survey process covers diesel engines, important shipboard pumps and other vital machinery. (Source: Wikipedia) Classification societies set technical rules based on experience and research, confirm that designs and calculations meet these rules, survey ships and structures during the process of construction and commissioning, and periodically survey vessels to ensure that they continue to meet the rules. Classification societies are also responsible for classing oil platforms, other offshore structures, and submarines. This survey process covers diesel engines, important shipboard pumps and other vital machinery. (Source: Wikipedia)

(d) safety systems – systems used to maintain the integrity, safety and/or security of the ship and its cargo.
(e) cargo systems – systems used to monitor and manage cargo directly.
(f) passenger management systems – systems used to provide services/facilities to passengers and to maintain the health and wellbeing of both passengers and crew.
(g) passenger/crew access systems – any systems provided for passenger/crew interaction that are not related to ship operations or passenger/crew management.

A.3.1 Communications

There are a number of on-board only, ship-to-shore and ship-to-ship communications systems that may be in use to meet a number of different requirements or to provide facilities for the Company, crew or passengers. Some of the more common systems in use are:

(a) satellite – a number of different applications use satellite communications for ship to shore communications covering both voice and data systems.
(b) VHF/UHF – communication systems using these frequency bands work on line of sight or general broadcast area communications and include marine VHF operating in the 156 to 162.025 Mhz range for ship to ship and ship to shore use, with different channel allocation depending on where the vessel is globally. VHF Channel 70 for example is used for digital selective calling (DSC), a paging system transmitting and receiving data calls for alerting purposes.
(c) S-Band – localised systems utilising the private allocation of the 2.4 Ghz and 5 Ghz frequency bands. Often used for Wi-Fi and Bluetooth applications.
(d) PABX/GSM 3G, 4G & 5G – these systems can be either locally provided or remotely connected if operating close to shore such as ferries. A local PABX or GSM base station may be deployed for use on cruise liners to provide both fixed and mobile phone access to passengers connected through the SatCom system to join the land-based infrastructure. A ferry might also utilise 4G aggregations to provide digital internet communication for passengers.

It is essential therefore that any and all communications systems are identified along with the various sub-systems that they may be connected to within all of the categories identified.

A.3.2 Navigation systems

There are a number of navigation systems and navigation aids that are in use and many of these systems interconnect to other systems on board, the primary ones that interconnects various subsystems are:

(a) Voyage data recorder (VDR), is a data recording system designed for all vessels required to comply with the IMO's International Convention SOLAS Requirements (IMO Res.A.861(20)) in order to collect data from various sensors on board the vessel. The data recorded in the VDR may include some or all of the following information types:

i position, date, time using GPS;
ii speed log – speed through water or speed over ground;
iii gyro compass – heading;
iv radar – as displayed or AIS data if no converter available for the Radar video
v ECDIS – a screen capture every 15 seconds and a list of navigational charts in use every 10 minutes or when a chart change occurs;
vi audio from the bridge, including bridge wings;

vii VHF radio communications;
viii echo sounder – depth under keel;
ix main alarms – all IMO mandatory alarms;
x hull openings – status of hull doors as indicated on the bridge;
xi watertight and fire doors status as indicated on the bridge;
xii hull stress – accelerations and hull stresses;
xiii rudder – order and feedback response;
xiv engine/propeller – order and feedback response;
xv thrusters – status, direction, amount of thrust % or RPM; and
xvi anemometer and weather vane – wind speed and direction.

(b) Electronic chart display & navigation system (ECDIS), an electronic chart system to pinpoint location and attain direction. This system may interconnect with such subsystems as steering, propulsion, autopilot, GPS and the ships Gyrocompass providing a central system from which others may be impacted. It should be noted that some of these systems are also in a different category providing a bridge capability. Other navigation systems or aids may include; Marine Radar, Automatic Tracking Aids, Echo Sounder, AIS, LRIT, GNSS, NavTex as well as navigation lights and the ship's whistle.

A.3.3 Ships plant systems

This is the largest category by far and includes the systems traditionally covered by the engine room including propulsion, steering, ballast, power generation and distribution, ventilation, lube oil, water (both waste and potable), etc. With the inclusion of the cruise ships we have to recognise that these floating hotels may also have the equivalent building management systems to control lighting, heating, ventilation and air-conditioning (HVAC), etc.

This is traditionally the ships equivalent of the Industrial Control Systems (ICS) that operated as stand-alone systems. With the addition of multiple sensors utilising a range of different signalling protocols the traditional SCADA system rarely exists in modern ships. It is not uncommon to find a mix of control protocols such as MODBUS working alongside systems that are starting to utilise the 'Industrial Ethernet' to provide connection and operational command and control.

Sensor data may also be used to provide data to more than one subsystem both within and external to the systems within the originating category, this indicates that these sensors have a higher criticality to the overall operation of the ship. A system may also have multiple sensors with the data being integrated and/or aggregated in some way to multiple data points on the operational status of the system.

A.3.4 Safety systems

A number of systems in this category are mandated by the SOLAS requirements, however this category includes any system that may have an impact on the safety or security of the ship, cargo, passengers and crew. Systems include; GMDSS (Global Maritime Distress & Safety System), AMVER (Automated Mutual-assistance Vessel Rescue), SSAS (Ship Security Alert System), NavTex, Radar, Sonar, Public Address & General Alarm Systems, Voyage Data Recorder, TeleMed, Fire etc.

Safety systems are often linked to the ships plant monitoring systems for activation when certain fault conditions are identified and the safety systems may be able to override the

operational systems in order to contain the danger to a particular area or to shut down a system in order to stop further damage.

Many of the safety systems are connected to the ship communication systems in order to alert other ships. This includes communications systems covering all frequency bands from SatCom to HF.

A.3.5 Cargo management systems

Different cargo management systems will be employed dependent upon the cargo type and class of ship. Tankers for oil or LPG will employ different cargo management systems to that of the container ship. These cargo management systems are not only for when loading or offloading but, for certain cargo, also provide a constant monitoring function during transit.

When the ships function is for that of carrying passengers, cargo management systems may also include the equivalent of an airport baggage handling system and certainly for ferries will include tracking systems for vehicles possibly connected to shore-based Automatic Number Plate Recognition (ANPR) systems.

A.3.6 Passenger management systems

Passenger management systems will increase in number and complexity with the number and duration of passengers on board. Passenger Management systems are used to provide services/facilities to passengers and to maintain the health and wellbeing of both passengers and crew.

The TeleMed system is included in this category as well as the safety systems category as it is quite likely on certain ships that the system may be used for general medicine dispensing, whilst at the same time it may hold passenger or crew medical records. Such a system will require careful consideration with regards to access control.

Other passenger management systems may include Point of Sale (PoS) systems for shops and restaurants, central booking systems for theatres and other venues, room allocation and management of other financial transactions.

Passenger management systems are those systems that will not be accessed directly by the passengers and only accessed by the crew who are responsible for using the systems on behalf of the passengers.

A.3.7 Passenger access systems

A passenger access system is any system where the passenger may access or interface directly with the system. This includes any system that allows the passenger to interface with a passenger management system via a portal for online booking or payment for services.

More generally these systems will include systems that provide access to multimedia services such as films or music and systems that allow connection to the Internet.

The category grouping provided is based on a number of considerations, including functionality of the system, relationship to other systems within the same category, operator/maintainer interaction and the underlying technology used.

Ships are very modular by design resulting in a common physical infrastructure to carry the mass amount of cable required to interconnect the sensors and equipment to the

operations and monitoring capability as well as providing physical infrastructure for power distribution. This common physical infrastructure also provides for wiring cabinets located around the ship that are used for patching and management of the cabling infrastructure used to support many of the ship systems. These common 'junctions for maintenance' provide an environment whereby cross system contamination/connection may occur either by negligence or malicious act. Good awareness, access control and configuration management is required to minimise any risk.

The desire to reduce manpower on-board has resulted in almost all of the systems being developed with some form of sensing to monitor the operational parameters of the systems and central command and control panels to provide not only centralised situational awareness but central locations where the systems may be operated from. These centralised command and control positions may have master and slave units to provide control from the bridge or at ancillary control points around the ship.

A.3.8 Systems interdependencies and architecture

Identification of the systems deployed or to be deployed have to be identified along with any system interdependencies either for operational reasons, access to communications or that they are using a common underlying infrastructure such as Industrial Ethernet or MODBUS. This will include all of the various sensors and sensor systems used either directly by the systems or to provide situational awareness of the operational status of the system.

Once the interdependencies and data or information exchange requirements are identified and understood, overall systems architecture can be developed that provides for the optimum security without the addition of additional technology. This especially includes ensuring that separation exists between systems where passengers do not require any access.

A.3.9 Access to systems

When identifying and categorising the systems that are deployed on board and identifying the interdependencies between them, it is important to also identify who requires access to the systems and for what purpose.

The ships natural hierarchy will assist in identifying who requires or should have access to the most sensitive systems on board and what controls should be put in place. As ships become more and more automated and complex the need to track access on all systems will increase in order to carry out any investigations, should an incident occur.

APPENDIX B

Process for developing a cyber security assessment (CSA)

Note: This Appendix addresses both the assessment of cyber security risks and the identification and prioritisation of risk treatments (security controls) so as to provide a basis for implementation of the measures through the cyber security plan (CSP).

The ship security officer (SSO) and the cyber security officer (CySO) should first assess each of the vulnerability and security controls identified in the ship security assessment report (SSA) to establish whether there are cyber security implications arising from them. For example, the deployment of technology-based security systems as security controls to specific security threats or vulnerabilities may introduce or increase cyber security vulnerabilities.

The SSO should then review the ship's overall business and operations to assess the level of exposure and whether there are any additional potential cyber-related threats and vulnerabilities, across the full range of ship systems and data (for example, navigation systems, cargo handling systems, passenger information systems, security systems, industrial control systems, etc.), not identified in the SSA, but which nevertheless impact on the cyber security of the ship.

Where the SSA does not cover the full range of potential cyber security threats, the SSO should produce a CSA. This CSA should cover and document the same aspects as the security assessments for a ship as described in Section 5.

The completed CSA may form an annex of the SSA for the ship.

B.1 Identification and evaluation of important assets and infrastructure

It will first be necessary to have an understanding of:

(a) how the different assets support the ship's operational use, both when underway and when in port or moored;
(b) the criticality of different areas within the ship and the assets/systems they contain; and
(c) the systems that operate in, support or protect these critical assets or areas.

From a cyber security perspective, the business and operationally critical and/or sensitive elements of a ship are likely to include:

(a) those assets that have been judged could be used to significantly compromise the integrity of the ship as a whole or the ability of a specific area or system to function as required. Consideration should be given to:

- **i** cabling routes and their containment (for example ducts and trunking);
- **ii** configuration, identification and use of control systems;
- **iii** critical permanent plant or machinery;

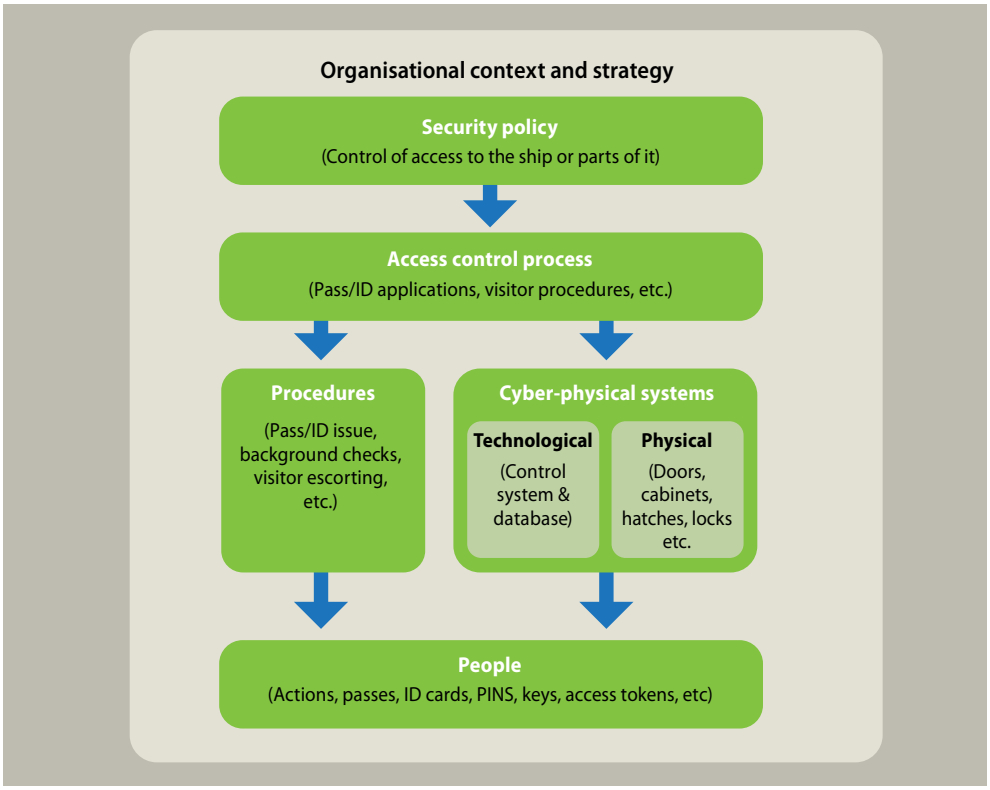
iv security or other control rooms, including guarding;
v security, alarm and access control systems, CCTV and video processing; and
vi key spaces and facilities used by law enforcement and security service personnel operating in, or visiting, the ship.

(b) ship data relating to the location, identification, technical specification and operation of business critical and sensitive assets;
(c) ship systems, wherever they are hosted, used for planning, scheduling and shipping operations; and
(d) assets or systems upon which the business critical and/or sensitive elements are dependent for their normal operation and resilience.

B.2 Identification of the ship business processes

The operation of a ship will depend on a set of business processes that rely upon ship data for the safe, secure and efficient operation and enable supporting processes such as asset management, resource scheduling, financial and business planning, procurement, and the human resource processes. Having identified and assessed the important assets and infrastructure, the next step is to identify the ship business processes that use the assets and infrastructure, as illustrated in Figure B.1

▼ **Figure B.1** Example of components supporting access control process



This understanding of the business processes should be used to assess the criticality of assets and to understand the interdependencies of the data and systems within the overall operational and business processes of the ship. By so doing, the real impact of failure or compromise of individual components can be understood.

B.3 Identification and assessment of risks arising from potential threats and vulnerabilities

The potential threats should have already been identified in the SSA and mitigated via the SSP. However, it will be necessary to understand the likely capability of each to impact on the cyber security of the ship and ship systems.

When considering threat scenarios and types of undesired event, the Company should include incidents such as:

(a) unauthorised access to sensitive ship data (commercial, personal or security-related);
(b) theft of sensitive ship data;
(c) deletion, unauthorised modification or corruption of ship data;
(d) infection with malware;
(e) loss of service from systems due to loss of connectivity or power;
(f) loss of service from systems due to software and hardware failures;
(g) compromise of ship security systems;
(h) denial of service – externally hosted systems;
(i) denial of service – ship systems;
(j) jamming or interference with positioning systems (GNSS/GPS); and
(k) assessing efficacy of system operation (for example coverage and performance of CCTV and intruder detection systems).

The identification of vulnerabilities should include consideration of:

(a) the relationships between systems;
(b) the technical composition of systems in terms of hardware and software components and the builds or revisions that are being used;
(c) physical robustness of enclosures (for example cabinets, ducts, trunking, etc.);
(d) the relationships between systems and associated business processes;
(e) existing security measures and procedures, including the presence and permeability of any secure perimeter that prevents or limits access to the ship, the ship systems and associated cargo, plant and machinery;
(f) reliance on automation of equipment;
(g) the level of resilience within the ship and ship systems, including the level of dependency of systems on external infrastructure and systems, for example, global satellite navigation systems for position and timing information;
(h) any conflicting policies between safety and security measures and procedures;
(i) any enforcement and personnel constraints; and
(j) any deficiencies identified during daily operation, following incidents or alerts, the report of security concerns, the exercise of control measures, audits etc.

The risk assessment should consider the nature of harm that may be caused to: the ship, shipboard personnel, passengers, other assets and personnel; and/or the benefits the ship exists to deliver, be they societal, environmental and/or commercial.

The cyber security risk will depend on the likelihood that a threat actor can exploit one or more vulnerabilities and cause the nature of harm identified.

B.4 Identification, assessment, selection and prioritisation of security controls

For every cyber security vulnerability not already identified by the SSA, the CySO should identify and record possible mitigation or security controls.

The assessment of each countermeasure should identify and record:

(a) the cost of the countermeasure and its implementation.
(b) other impacts which the countermeasure might have, for example, on asset or system usability and efficiency, business processes and ship operations.
(c) wherever possible, to support the business justification for investment in the countermeasure:

- **i** the risk reduction which could be achieved; and
- **ii** the predicted cost saving or loss reduction.

(d) the potential for the countermeasure to create further vulnerabilities.
(e) whether the countermeasure delivers any other business benefits, for example:

- **i** reduction of overall business risk; and
- **ii** aiding the development of efficient, robust and repeatable business processes.

The security controls that are chosen for implementation should be appropriate and proportionate to the risk they are intended to mitigate. The selected measures should be listed in the CSA and form the basis of the CSP.

B.5 Review acceptability of overall risk

The assessment process should continue until a point is reached where the level of residual risk does not exceed the risk appetite of the Company, i.e. repeat the steps outlined in Sections B.3 and B.4. The remaining residual risks should be listed in the CSA.

B.6 Review of the CSA

As with the SSA, the CSA should be periodically reviewed and updated, taking account of:

(a) changes in previously identified risks;
(b) new threats or vulnerabilities;
(c) changes to the ship or its use;
(d) the success of implemented security controls; and
(e) new and, potentially more effective, security controls.

The Company should establish a suitable mechanism for performing ad-hoc risk reviews to identify and assess the impact of any changes on the ship that should be reflected in the CSA. The triggers for initiating such a review and the timetable for its completion should be set out within the CSP. Triggers should include as a minimum the following events:

(a) a significant security incident at a port or port facility;
(b) a significant security incident affecting an externally hosted ship system;
(c) a change in the shipping operations undertaken by the ship;

(d) a change in the location, hosting or support of ship systems;
(e) a project initiated to significantly change the ship or its operations;
(f) a change of ownership or operating company; and
(g) a significant security incident at sea.

Where the ship contains a number of functions, areas or assets with different risk profiles, the CSA may need to be reviewed at a higher frequency in relation to any aspects that are deemed to be more sensitive. It is especially true of cyber security that any risk assessment represents a snapshot at a particular instance and which may change dramatically with the emergence of a new vulnerability.

APPENDIX C

Contents of a cyber security plan (CSP)

The ship security standards define the term 'security level' to mean the degree of risk that a security incident will occur or be attempted. The CSP needs to be developed to cover the three security levels specified in the ISPS Code.

The recommended contents of the CSP should include, as a minimum:

(a) information on cyber security responsibilities and links to organisations that will assist the ship in the event of a cyber security incident.

Note: See Table 7.1 in Section 7.1 regarding the issue of legal jurisdiction in the event of a significant cyber security incident requiring government assistance.

(b) how the cyber security of communications, navigation and other critical systems and equipment will be maintained.
(c) the cyber security drills to be practiced to test the ship's and shipboard personnel's response to cyber security incidents.
(d) the cyber security of communications, including those:

- **i** between personnel with security responsibilities;
- **ii** between those responsible for technical security and the wider security team; and
- **iii** providing information about the ship and ship assets to third parties.

(e) cyber security measures required for any connection between ship systems and those of any port or port facility it visits, or for ship-to-ship activities – connection to another ship.
(f) processes and procedures for approving the electronic or wireless connection of ship and ship systems.
(g) any changes to systems or system operations required at higher security levels, including any increased security measures required for admission of IT and systems maintenance contractors to the ship when it is operating at security levels 2 and 3.
(h) access control measures relating to cable ducts, trunking, equipment compartments or cabins and equipment boxes, irrespective of whether they are located in restricted or open areas aboard the ship.
(i) access control measures relating to sensitive IT systems and accommodation, for example spaces containing networking, communications and server rooms.
(j) cyber security measures pertinent to the protection and assurance of cargo-related data and the systems that process, store and transmit it. Where the ship has automated systems handling cargo movement or storage, the plan should address the security measures required to protect the operational IT and cyber-physical systems.
(k) cyber security measures pertinent to the protection and assurance of ships stores and bunkering data and any systems that process, store and transmit it.
(l) cyber security of ship lighting, electronic access, security and monitoring systems, and any specialist systems required to support its safe and secure operation.

(m) response to cyber security threats, breaches and security incidents.
(n) arrangements for auditing of cyber security measures.
(o) contractual measures for the adoption of relevant cyber security measures within the supply chain to the ship.
(p) cyber security awareness and training required by shipboard personnel and personnel within the ship's supply chain.

The section of the CSP addressing security breaches and incidents should enable an effective and coordinated response. This will require an assessment of potential risks to the ship, its function, ship assets, personnel and third parties in the event of a security breach or incident. The section should include:

(a) the risk mitigation measures including:

- **i** the forensic readiness measures required to enable, when required, the capture of forensic information about an incident for use by law enforcement, and/or detailed analysis of the root causes of the incidents;
- **ii** the process to be followed on discovery of a breach/incident (including near misses, i.e. narrow avoidance of a security breach/incident);
- **iii** business continuity measures required in the event of ship system failure, impairment or non-availability;
- **iv** the disaster/incident recovery actions required in the event of serious failure scenarios; and
- **v** steps to be taken to contain and recover from the event.

(b) the review process to be followed following a security breach or incident, including both assessment of any on-going risk and evaluation of the response to the breach or incident by the SSO and where appropriate the supply chain.
(c) the need for contractual provisions to handle breaches/incidents caused by a third party connected to the ship, for example, a professional advisor, contractor or supplier.
(d) the mechanisms for reviewing and updating the CSA, CSP and security procedures following a significant security breach or incident affecting:

- **i** the ship; or
- **ii** another ship in the fleet; or
- **iii** another ship of the same or similar class.

(e) the arrangements for shipboard personnel to implement in conjunction with existing business continuity planning and exercises.

APPENDIX D

Devising mitigation measures

This Appendix provides a framework for the identification of mitigation measures to be applied to the people, physical, process and technological aspects of a ship. When choosing mitigation measures, a balance will need to be struck on a case-by-case basis between optimum risk reduction and minimising the overall impact on the operation of the ship.

D.1 People

People are often the weakest element in any secure system or operation so the interaction of people with the ship systems needs to be understood. It is therefore advised that the answers to the following questions are established as the first stage in the process of deciding upon the mitigation measures which are appropriate and proportionate:

(a) who needs access to the ship data and systems?
(b) what types of access are required?
(c) how is this access provided, and is it required remote of the ship?
(d) what access controls will be required (for example, can an individual create, read, update or delete the ship data, and what level of control does an individual have)?
(e) what level of cyber security awareness and understanding of cyber security is required by individuals?
(f) are contractors, temporary and agency staff provided with cyber security awareness training as part of their induction?
(g) do individuals understand the ship operator's policies, processes and procedures for the creation, use and maintenance of ship data and the operation and maintenance of ship systems?
(h) are processes and procedures in place to update individuals about any changes in policies, processes and procedures?
(i) are individuals briefed in a timely manner on changes in threats, risks and the required security controls?

The answers to the first four questions will also enable the SSO to identify high-risk positions. The individuals holding those positions should be subjected to appropriate pre-employment/pre-contract security screening and vetting checks, with appropriate on-going monitoring.

High risk positions will include those with:

(a) IT and/or operational system administration responsibilities;
(b) security roles;
(c) information management roles;
(d) purchasing, finance and contract management roles; and
(e) personnel managers (regarding handling of security breach related disciplinary matters and management of the insider threat).

D.2 Physical

In order to enhance the achievable level of cyber security, it is necessary to have in place physical security which:

(a) prevents unauthorised access to sensitive ship systems, for example:
- **i** IT equipment accessing, processing or storing sensitive information;
- **ii** systems fulfilling safety critical functions; and
- **iii** security and control systems.

(b) prevents theft of, or damage to:
- **i** IT equipment, storage media, cables, etc.; and
- **ii** ship data, in particular that pertaining to the safe and secure operation of the ship.

(c) protect network and communications infrastructure from:
- **i** accidental damage;
- **ii** deliberate/malicious damage; and
- **iii** tampering and/or denial of service.

(d) protect utilities, heating, ventilation and cooling systems required to:
- **i** operate the sensitive ship systems;
- **ii** operate the network and communications infrastructure; and
- **iii** maintain a safe and secure working environment.

Some ship systems may need to be accorded the same level of physical protection as key operational spaces, with security perimeters defined and implemented to protect not only the systems but also their cabling and any associated power, plant and machinery.

It will therefore first be necessary to establish:

(a) what physical and electronic infrastructure is used to create, access, process and store ship data, including any communications and networking components;
(b) the infrastructure that is critical to ensure the ongoing operation of ship systems and any processes or services they support;
(c) the dependencies that parts of the infrastructure have on other critical services or infrastructure;
(d) the extent to which this infrastructure is dedicated to ship systems or shared with different activities;
(e) the extent to which this infrastructure is shared with third parties; and
(f) availability of personnel and external agencies for reaction and response and their ability to access the functional areas.

This information should then be used to decide where physical protective measures are required.

Where it is decided that secure perimeters are needed, these should be designed to prevent unauthorised access or tampering and, depending on the location and criticality, may need to be alarmed and monitored by CCTV systems. When considering the level and type of protection to be provided, a defence in depth approach is more reliable than a single protective barrier.

D.3 Process

The failure to develop and maintain appropriate policies and their supporting processes that reflect the operating culture of the organisation can result in them being ignored, or lead to the adoption of informal local practices, resulting in the security or operation of the ship assets being undermined.

It is therefore important that processes specific to cyber security are in place which, as a minimum, detail:

(a) the use of externally hosted systems or business portals employing web-based interfaces;
(b) communications and networking links, whether from externally hosted systems or services, or those hosted at a port or port facility that the ships is visiting;
(c) wireless networking and communications technologies, for example Bluetooth and Wi-Fi;
(d) configuration of protective software, such as firewalls, anti-malware products and intrusion detection applications;
(e) the connection of new computers, mobile devices or IT-controlled operational equipment to the ship's IT infrastructure;
(f) the use of personal mobile radios (PMR) aboard the ship;
(g) configuration and management of user and systems account privileges, including those of third party personnel, with access to ship systems particularly those controlling power, heating, ventilation and cooling systems for accommodation containing on-site IT systems, or ship security systems, for example, access control, security barrier control, CCTV, etc.;
(h) connection of personal IT devices or removable media to ship systems;
(i) access to emails, instant messaging services, external websites or file sharing services from workstations on operational systems (control systems, security systems, etc.); and
(j) mobile time-critical access to data during an emergency.

It will also be necessary to have processes in place for:

(a) regularly reviewing access privileges to ensure that individuals' privileges are consistent with their job roles and functions; and
(b) regularly reviewing systems logs and the investigation of anomalies.

D.4 Technological

In deciding upon technical mitigation measures that are needed to address cyber security risks, it will first be necessary to gain an understanding of:

(a) the systems in use;
(b) the channels used by systems, sensors and actuators to communicate; and
(c) the information and data held.

Systems may operate throughout the ship or may be limited to specific areas. They may be located entirely on board, hosted by the Company or operate remotely, for example, the provision of satellite navigation signals. In order to establish the nature of systems in use, the following questions will need to be answered:

(a) what ship systems are involved in the creation, use, maintenance, storage and transmission of ship data?

(b) to what extent are each of these systems dedicated to a single ship?
(c) are the ship systems shared by different activities?
(d) are the systems accessible by any third parties, aboard the ship, ashore, or on another ship?
(e) what is the typical operating life of each system?
(f) when is it likely that each system will become unsupportable, obsolete or need to be replaced for business and/or operational reasons?

The channels by which systems, sensors and actuators communicate may be vulnerable to attacks and interference. The answers to the following questions should therefore be sought:

(a) what channels, technologies and parts of the overall spectrum are used to communicate and share ship data between ship systems and with any users who need to access or use it?
(b) what channels, technologies and parts of the electro-magnetic spectrum are used to control and integrate ship systems?
(c) to what extent are the communications confined to the ship, and will remote access to, or remote processing of, communications be required?

The information and data that is created used and/or processed by the ship systems needs to be understood. In order to do this, the answers to the following questions should be established:

(a) what information and data, including sensor data, do the ship systems require to function?
(b) what other information and data is held, for example, personally identifiable information?
(c) what legal requirements are there with regards to the information and data held?
(d) how are information and data encoded?
(e) how and where are information and data stored?
(f) how are the data/information to be protected whilst at rest, in transit or in use?
(g) what will the consequences be if information and/or data was lost and therefore no longer available?
(h) who owns the information and data?
(i) how are information and data made available and what restrictions are there on their use?
(j) how long do information and data need to be kept?
(k) what information and data need to be securely removed when no longer required?

When designing, procuring, implementing and operating physical security systems that operate over IT, the SSO should consider how the systems will be protected from cyber security attacks or incidents. This is particularly important given the trend of convergence of system, for example, the use of a shared network carrying operational data, administrative data and personal email traffic from shipboard personnel.

Where such convergence occurs, or has occurred, the Company should ensure that:

(a) an appropriate architecture is employed;
(b) appropriate management, support and maintenance is available from both the ship's engineering teams and the system vendors, to maintain system security and performance;
(c) appropriate protection is provided to prevent IT control and security systems becoming infected with malware;

(d) wherever possible the critical security systems operate over a segregated infrastructure; and
(e) where appropriate encryption technology should be used to protect the data/ information whilst at rest, in use or in transit.

D.5 Resilience

Resilience is the ability to adapt, respond and recover rapidly from disruptions and maintain continuity of business operations.

In the event of an incident it is vital, from a business perspective, that a ship is able to operate without disruption or compromise of the services provided to its users.

A ship should therefore have in place an incident management plan which is based upon an understanding of:

(a) the potential causes of disruption, cyber, human and natural;
(b) the essential systems required to keep the ship operating safely;
(c) the nature and practicality of alternative methods which can be employed in the event of an incident to maintain operations; and
(d) the capacity at which the ship can realistically operate under such arrangements.

It will also be necessary for the ship to have in place systems and processes which enable the timely detection of disruptive events in order to enable the correct response, as set out in the incident management plan, to be initiated as quickly as possible.

Emergency plans should be exercised on a regular basis, to test communication, coordination, resource availability, procedures and response. The exercises may be:

(a) full-scale or live;
(b) table-top simulation or seminar; or
(c) combined with other exercises such as emergency response, etc.

APPENDIX E

Handling release of information to third parties

There are a number of situations where a ship may be asked or required to publish information about its plans and operations. These may include release of information to regulators, investors, insurers and presentations about the ship(s). The Company and ship's master needs to be aware the public release of information may enable a party undertaking hostile reconnaissance to obtain sensitive information or through data aggregation to deduce sensitive information.

Where a ship falls within the scope[1] of regulations or legislation requiring public disclosure of information, including responses to requests made under Environmental Information Regulations or Freedom of Information legislation, the Company should ensure that the CSP details the approach to be taken to protect sensitive data or information. As a minimum the approach should:

(a) consider the impact of releasing data, including the potential issues arising from data aggregation;
(b) prevent leakage of security-related information;
(c) protect commercially sensitive data and intellectual property; and
(d) safeguard personally identifiable information, taking into account the range of attributes that can be used to identify individuals.

Based on an assessment of the risk of disclosing detailed information about the ship, it might be necessary and appropriate to adopt measures to reduce the detail and granularity. Measures that might be necessary include, but are not limited to:

(a) limiting access to particular types of ship data;
(b) redacting sensitive information, for example, description of the functions of individual ship systems or components of them; and
(c) providing the information in an unstructured format, for example, hard copy, images or non-interactive PDF formats.

---

1 The scope will be determined by the nature of the relationship between the ship and the public sector organization, for example, if it is owned, operated, leased, chartered or contracted for use by the public sector organisation.

APPENDIX F

Handling security breaches and incidents

Note: The references in this section to reporting to UK authorities are applicable to British ships, those ships with substantial operations in British waters and actions of individuals where UK courts have jurisdiction over any related cyber security incident (see Section 7.1). For ships and/or individuals that fall outside of this scope the CySO or CSO should report the incident to the relevant national authorities.

It will be necessary for a ship to have in place appropriate measures that may be implemented in the event of an incident to reduce its impact on the ship's operations and aid recovery. These are likely to include:

(a) incident response plans, which include liaison, where appropriate, with UK Law Enforcement, the UK's National Cyber Security Centre (NCSC)[1], UK CiSP, DfT and Action Fraud[2];
(b) communication plans to reassure and inform stakeholders, during and after any incident or breach, as well as handling any third party, regulator, media or public interest issues;
(c) risk assessment and mitigation plans to enable the impact to be assessed over both the short and medium to longer terms; and
(d) disaster recovery and business continuity plans which are able to afford the same level of security for the ship data as the processes and systems in use on a day-to-day basis.

It will also be necessary for consideration to be given to when and how forensic evidence will be preserved to aid in any investigation into the cause of the event or the perpetrators. Where evidence collection is for law enforcement purposes it should be in accordance with the relevant national guidelines[3;4].

---

1 NCSC [https://www.ncsc.gov.uk] has four main responsibilities that flow from the UK's Cyber Security Strategy:
- **(a)** to understand the cyber security environment, share knowledge and use that expertise to address systemic vulnerabilities;
- **(b)** to reduce risks to the UK by working with public and private sector organisations to improve their cyber security;
- **(c)** to respond to cyber incidents to reduce the harm they cause to the UK;
- **(d)** to nurture and grow our national cyber security capability, and provide leadership on critical national cyber security issues.

2 Action Fraud is the national reporting service for fraud and cyber crime. It covers police forces in England Wales and Northern Ireland, taking reports via its call centres or website. You can report the incident using Action Fraud's online fraud reporting tool (http://www.actionfraud.police.uk) or call 0300 123 2040.

3 In the UK these are the ACPO Good Practice Guide for Digital Evidence (2012), which is available from https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

4 CESG, Good Practice Guide Forensic Readiness, October 2015, Issue 1.2 [https://www.ncsc.gov.uk/content/files/guidance_files/GPG%2018%20-%20Forensic%20Readiness%20-%20Issue%201.2%20-%20Oct%2015%20-%20NCSC%20Web.pdf]

In the event of an incident involving the loss or theft of ship data, unauthorised access to ship data or systems, or interference with computer systems, the CSO or CySO should notify the relevant parties[5] and law enforcement agencies.

When personally identifiable information is lost, stolen or compromised, the CSO or CySO should ensure that the relevant information commissioner or data protection authority[6] and affected individuals are notified.

The CSO or CySO should ensure that discovery procedures are established in all appointment documents and contracts, including, where applicable, in non-disclosure agreements.

Following any security breach or incident, an important post-incident activity is the formal evaluation of the way that the event was handled, to determine lessons that can be learned and to review whether any changes are required to the security assessments, security plans or supporting policies, processes and procedures.

Regular exercises at the Board and ship levels should be carried out to simulate a cyber incident allowing for those who make the decisions to understand and be aware of the impact such an incident may have.

5 In the UK jurisdiction (see 7.2.8), significant incidents affecting ships or ports covered by the ISPS Code or ILO/IMO CoP should in the first instance be notified to the NCSC, otherwise they should be reported to the CiSP and Action Fraud.

6 For incidents involving the loss or compromise of personally identifiable data from a British ship, the CSO or CySO should notify the Information Commissioner's Office (http://www.ico.org.uk).

APPENDIX G

Supply chain security

Ships, as complex cyber-physical systems, are vulnerable to cyber security incidents emanating from the supply chain that supports them, both when in operational use and when undergoing major maintenance or refits. The Company should be aware of this risk and consider what steps are prudent to protect the ship and its systems.

When developing the CSP, the CySO should consider what security-minded measures are required. Aspects that might typically be addressed at a generic level in the plan in respect of suppliers are:

(a) good governance – clear security responsibility and accountability within the supplier's organisation, up to and including senior management/board level.
(b) security culture and awareness – the adoption and promotion of a good security culture with a programme to maintain awareness.
(c) risk management – evidence of the existence and use of polices, processes and procedures to manage not only safety risks, but also security risks.
(d) information security – the identification and handling of sensitive information regarding the ship, or ships.
(e) technology and services – the cyber security requirements for systems storing or processing ship or Company information and where the technology will be used on board the ship or remotely connected to the ship systems, the cyber hygiene requirements.
(f) personnel security – the measures to be applied to personnel who will be working on board the ship or providing operational support to it. These measures may mirror those in use for the Company and ships personnel or may vary according to the role(s) fulfilled.
(g) physical security – the measures to be employed to protect sensitive information, components, software, and any shore-based systems providing support or services to a ship.
(h) handling of security incidents – the mechanisms managing security incidents, including 'near-misses', and the arrangements for reporting any incidents to the CySO and the Master or Captain of any affected ships.

The cyber security measures required in point (e) above may be determined by assessing the level of threat and potential impact the supplier could have on critical or sensitive ship systems. A tiered approach may be adopted using supplier risk profiles as illustrated in Table G.1.

Table G.1 Profiling cyber security threat to a supplier

Threat profiles	Description of cyber threat to supplier	Mitigation approach
Very low	Basic, untargeted threat, e.g. accidental malware infection due to poor cyber hygiene.	Supplier to obtain and maintain Cyber Essentials certification
Low	Basic, but more targeted threat, e.g. phishing attacks on supplier to infect or gain access to supplier's systems.	Supplier to obtain and maintain Cyber Essentials Plus certification
Moderate	Tailored and targeted, attempts to gain access to specific assets or information.	As Low, plus robust policies in place to cover all topics in G.2
High	Highly sophisticated, well-resourced attacker seeking to gain access to specific assets or information.	As Moderate, but additional technical controls, for example use of intrusion detection system (IDS) and data loss prevention (DLP) tools. Regular penetration testing to proactively verify effectiveness of controls.

APPENDIX H

Bibliography

The Appendix lists standards that are relevant to the design and operation of information and communications systems used in the management and operation of the ship.

H.1 General IT and cyber security standards

Reference	Title/Description
ISO/IEC 13335	*IT Security Management – Information technology – Security techniques – Management of information and communications technology security*
ISO/IEC 15408	*Common Criteria for Information Technology Security Evaluation*
ISO/IEC 27001	*Information security management systems – Overview and vocabulary*
ISO/IEC 27001	*Information security management systems requirements*
ISO/IEC 27002	*A code of practice for information security management*
ISO/IEC 27003	*Information security management system implementation guidance*
ISO/IEC 27004	*Information security management – Measurement*
ISO/IEC 27005	*Information security risk management*
ISO/IEC 27006	*Requirements for bodies providing audit and certification of information security management systems*
ISO/IEC 27007	*Guidelines for information security management systems auditing*
ISO/IEC TR 27008	*Guidance for auditors on ISMS controls*
ISO/IEC 27010	*Information security management for inter-sector and inter-organizational communications*
ISO/IEC 27013	*Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*
ISO/IEC 27014	*Information security governance*
ISO/IEC 27017	*Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
ISO/IEC 27018	*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
ISO/IEC 27031	*Guidelines for information and communication technology readiness for business continuity*
ISO/IEC 27033-1	*Network security – Part 1: Overview and concepts*
ISO/IEC 27033-2	*Network security – Part 2: Guidelines for the design and implementation of network security*
ISO/IEC 27033-3	*Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues*

Reference	Title/Description
ISO/IEC 27033-5	*Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*
ISO/IEC 27035	*Information security incident management*
ISO/IEC 27036-3	*Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*
ISO/IEC 27037	*Guidelines for identification, collection, acquisition and preservation of digital evidence*
Critical Security Controls	*Critical Controls Version 5.0 – 27 February 2014* A reference set of recommendations for methods to address risks to enterprise data and systems. Published by the Center for Internet Security (for further information, see https://www.cisecurity.org)
HMG IA Standard No 1	Technical Risk Assessment – IA Standard for Risk Managers and IA Practitioners responsible for identifying, assessing and treating the technical risks to ICT systems and services handling HMG information.
Supplier Information Assurance Assessment Framework and Guidance	Guidance on how the Supplier Information Assurance Tool (SIAT) question sets and tool specification can be used by suppliers of key business services to HMG.
Supplier Information Assurance Tool (SIAT) – Summary	A brief summary of the Supplier Information Assurance Tool (SIAT) Community of Interest set up to drive development of a supplier Information Assurance model. ISAB Approved.
BIS/12/1120	*10 Steps to cyber security: executive companion.* Provides guidance for business on how to make their networks more resilient and protect key information assets against cyber threats.
BIS/12/1121	*10 steps to cyber security: advice sheets.* Provides detailed cyber security information and advice on the 10 steps described in BIS/12/1120.
	Cyber Essentials Requirements Provides guidance on the most basic technical controls an organisation should have in place.
	Cyber Essentials Scheme: Assurance Framework Explains how the independent assessment process works and the different levels of assessment. It also provides guidance for security professionals carrying out the assessments.

H.2 Security and safety of Industrial Control Systems (ICS & SCADA)

Reference	Title/Description
IEC TS 62443-1-1	*Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*
IEC 62443-2-1	*Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*
IEC TR 62443-2-3	*Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment*
IEC 62443-2-4	*Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*
IEC TR 62443-3-1	*Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems*
IEC/TS 62443-3-2 Ed. 1.0	*Network and system security – Part 3-2: Technical requirements – Target security levels*
IEC 62443-3-3	*Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*
ANSI/ISA-99.00.01	*Part 1: Terminology, Concepts, and Models*
NIST IR 7176	*System Protection Profile – Industrial Control Systems – V1.0 Incorporates industrial control systems into Common Criteria*
NIST SP 800-82	*Guide to Industrial Control Systems (ICS) Security*
IEC 61508	*Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*

H.3 Business-related security guidance

Reference	Title/Description
BIS/12/1119	*Cyber risk management: a Board-level responsibility.* Explains the benefits of cyber risk management to senior executives.
ISO 20000 BS 15000	*IT Service Management Standards* based on ITIL.
BS 7858	*Code of Practice for Security Screening of Individuals Employed in a Security Environment*
COBIT 5	*A Business Framework for the Governance and Management of Enterprise IT* (Control objectives for information and related technology.)
PAS 555: 2013	*Cyber security risk. Governance and management. Specification*

H.4 Other standards and guidance

Reference	Title/Description
PCI DSS	*Payment Card Industry Data Security Standard*
NIST SP 800-61	*Computer Security Incident Handling Guide*
PAS 1192-5: 2015	*Specification for security-minded building information modelling, digital built environments and smart asset management*
PAS 754: 2014	*Software Trustworthiness. Governance and management. Specification*
PAS 97: 2012	*A specification for mail screening and security*
RFC 2196	*Site Security Handbook* From IETF (The Internet Engineering Task Force)
RFC 2350	*Expectations for Computer Security Incident Response* From IETF (The Internet Engineering Task Force)
BS ISO/IEC 42010	*Systems and software engineering – Architecture description*
	EACOE Enterprise Framework
	IET Code of Practice for Cyber Security in the Built Environment

APPENDIX I

Implementation checklist

Cyber security assessment (CSA)	
A CSA builds upon existing security assessments whenever appropriate to comply with the Ship Security Standards. The purpose of a CSA is to identify vulnerabilities in the cyber protection of ship systems, personnel security systems and business processes that may lead to a security incident affecting the ship, its crew, passengers or cargo.	
Yes/No	
	Have the ship's Master and Engineering Officer read the Code of Practice for Cyber Security of Ships? Have you considered it in your ship's business continuity plans?
	Have you considered security-related standards and best practice guidance that apply to Information Technology (IT), Operational Technology (OT) and Communications systems, including those used for the propulsion, steering and navigation of your ship? [See Appendix H of the Code of Practice document for further references to standards and resources]
	Has your ship developed a Cyber Security Assessment (CSA)? [See Appendix B of the Code of Practice document for further details]
	Does your CSA include:
	Identification of ship assets Identification and evaluation of important assets and infrastructure, e.g. functions, systems and data, that are considered to be important to protect, and external services, connectivity or data upon which the ship depends? The criticality of different functions and systems within the ship and their interactions and dependencies.
	Identification of ship business/operational processes Have you identified the ship's business and operational processes that use the assets and systems? The aim is to assess the criticality of assets and understand any on-board and external dependencies of the ship's data and systems within the overall business and operational processes, when underway, in port or moored.
	Identification and assessment of risks Have you identified and assessed the risks arising from potential threats (e.g. theft of sensitive data or infection with malware) to the assets and systems, the ship's vulnerabilities (e.g. the relationships between ship's functions and systems, including the reliance on automation of critical functions), and the likelihood of the risks occurring, so to establish the need for and prioritise security measures?
	Identification and assessment of security controls Have you identified, assessed, selected and prioritised appropriate and proportionate security controls and/or procedural changes, based on their costs, the level of effectiveness in reducing the relevant risk(s) and any impact upon the ship's operations? Are the security controls listed in the CSA, including any record of where cooperation or assistance is required from personnel or organisations that are not on-board the ship?

	Review acceptability of overall risk Taking into account the selected security controls, has the overall residual risk to the ship been identified and is it acceptable? Are the remaining residual risks listed in the CSA? Are the arrangements defined and in place for handling security breaches and incidents, whether they occur accidentally or deliberately?

Cyber security plan (CSP)	
Security assessments form the basis of security plans for ships and ship systems. A CSP should address issues identified in the relevant assessments by establishing appropriate security measures (designed to minimise the likelihood of a security breach as a consequence of potential risks).	
Yes/No	
	Has your ship developed a Cyber Security Plan (CSP), which builds upon the existing Ship Security Plan (SSP) wherever possible? [See Appendix C of the Code of Practice document for further details, including the three levels of risk the CSP should address (security levels 1 to 3), the recommended contents of the CSP and risk mitigation measures]
	Does your CSP take a holistic approach, covering people, process, physical and technological aspects of the ship's assets?
	Is your completed CSP protected from unauthorised access or disclosure?
	Has your completed CSP been turned into an annex of your SSP?
Does your CSP contain or reference:	
	The policies that set out the security-related business rules derived from the relevant CSP?
	The processes that are derived from the security policies and that provide guidance on their consistent implementation throughout the lifecycle and use of the ship's assets?
	The procedures that comprise the detailed work instructions relating to the repeatable and consistent mechanisms for the implementation and operational delivery of the processes?
	Have appropriate mitigation measures been developed to ensure optimal risk reduction while minimising the overall impact on the business and operation of the ship?
Review of the CSP	
	Is there a suitable mechanism in place for performing both ad hoc and periodic (at least annual) risks reviews to ensure the CSP remains fit for purpose, i.e. by addressing any identified gaps, organisational or operational changes that have arisen for political, economic, social, technological, legal or environmental reasons that impact the ship or its assets?
Monitoring and auditing of the CSP:	
	Does the CSP set out appropriate and proportionate monitoring and auditing measures that will be undertaken by suitably qualified and experienced personnel?
	Is the CSP aligned with the operational use of the ship and do the monitoring and auditing measures address the potential changes in risk environment over the life of the ship and its assets?

In respect of the monitoring and auditing measures:	
	Have you assessed the implementation of all security policies, processes and procedures affecting the ship and its assets, including the handling and storage arrangements for security sensitive items and data?
	Have you assessed the compliance of the ship's supply chain with the security policies, processes and procedures specified in the CSP, at a minimum on a risk-based sampling approach?
	Have you assessed the management of security controls that operate throughout the operational life of the ship, its assets and systems?
	If your ship has delegated some responsibility for compliance to a supplier, have you identified who is accountable for ensuring the overall effectiveness of the security measures and/or controls?
The CSP should detail:	
	The arrangements for maintaining senior security accountability within the ship and the Company
	Management of security responsibilities within the ship's supply chain, including: **(a)** the requirement for security responsibility to be retained at a senior level with suppliers' organisations; **(b)** appropriate delegation on a day-to-day basis to ensure effective operation of security processes and procedures; and **(c)** addressing legal jurisdiction issues where international suppliers are used and service delivery may be in a foreign port/waters or whilst the ship is underway in international waters.
Resilience:	
	To respond, adapt and recover rapidly from incidents or disruption, and to maintain the ships operations, does the CSP contain an incident management plan that is based on an understanding of: **(a)** the potential causes of incidents or disruption; **(b)** the critical systems required to safely operate the ship; **(c)** the nature and practicality of alternative methods that can be employed to maintain operations in the event of an incident; and **(d)** the capacity of the ship's functions and systems to safely operate under such arrangements.
	Does the ship have in place systems and processes to enable timely detection of disruptive events, to enable a prompt and effective response as set out in the incident management plan?
	Does the ship regularly exercise emergency plans (e.g. full scale/live, table top simulation or seminar) to test communication, resource availability, procedures and the effectiveness of the response?

Managing cyber security plan	
Following creation of the CSA and CSP, it is important that appropriate management arrangements are in place.	
Yes/No	
	Have you identified the individual responsible for the cyber security of the ship? (CySO) *A CySO is responsible for ensuring the development and maintenance of the CSP, and for implementing and exercising it*

	If your ship is part of a fleet, is there a Fleet Security Committee (FSC) or if not are there plans to create one?
	Does your ship have a security operations centre, either on-board or ashore?
	Does the ship have processes and procedures in place for the provision of sensitive information to third parties to prevent the risk of unauthorised disclosure of sensitive information? (See Appendix E of the Code of Practice for further information)
	Have you considered the arrangements necessary for managing security incidents or breaches? (See Appendix F of the Code of Practice for further information)
	Are you aware of the diverse range of threat actors that could be involved in a cyber security incident? (See Section 2 and Appendix A of the Code of Practice for further information)

IET Standards

Code of Practice
Cyber Security for **Ships**

The maritime sector forms a vital part of the UK economy, and as the complexity and connectivity of ships increase, ensuring their security and resilience is becoming more and more important. Poor security can lead to significant loss of customer or industry confidence especially where safety issues or financial losses are involved. To help senior shipping personnel who have responsibility for the on board security of a range of ships' systems, the Institution of Engineering and Technology (the IET) has worked in close association with the Department for Transport (DfT) and the Defence, Science and Technology Laboratory (Dstl) to produce this new code of practice.

This document provides actionable good practice advice on areas such as:

- Developing a Cyber Security Assessment and Plan
- Devising the most appropriate mitigation measures
- Having the correct structures, roles, responsibilities and processes in place
- Managing security breaches and incidents
- Highlighting the key national and international standards and regulations that should be reviewed and followed

This new code will be of real value to all those responsible for ship security and business continuity and can be used as an integral part of an organisation's overall risk management system.

www.**theiet**.org/standards

IET Standards
Michael Faraday House
Six Hills Way
Stevenage
Hertfordshire
SG1 2AY