LOSS PREVENTION Briefing

NORTH SERVICE, STRENGTH, QUALITY

LOSS PREVENTION BRIEFING FOR NORTH MEMBERS GENERAL / APRIL 2012

Ship Security

Contents

Introduction 1
ISPS Code 2
Security Assessment 2
Company Security Officer (CSO) 3
Ship Security Assessment (SSA) 3
Ship Security Plan (SSP) 3
Ship Security Officer (SSO) 4
Declaration of Security (DOS) 4
Training and Drills 4
Records 4
International Ship Security Certificate 4
Ship's Equipment 5
Management Systems 6
Control and Inspection of Ships in Port 6
Security of People on Ships 7
Practical Advice to Ship Operators 7
P&I Cover - Frequently Asked Questions 9

Introduction

Seafarers and ships have faced threats to their security ever since sea trade began. Over the past few years, robbery and piracy incidents have continued to occur and are very common in some parts of the world, such as off the coasts of Somalia and West Africa. Lack of security in port areas has also made it difficult for ships to prevent stowaways or the theft of cargo. Until 2001, ship operators and seafarers were often left to face these problems alone with little help from the authorities ashore. Terrorism was not seen as a significant maritime threat, especially to cargo ships.

The terrorist attacks that did occur against merchant ships were generally directed against passenger or cruise ships, such as the attacks on the Achille Lauro off Egypt in 1985, and the City of Poros in Greece in 1989.

Following the Achille Lauro incident, the Maritime Safety Committee (MSC) of the International Maritime Organization (IMO) adopted a set of security guidelines, which were published in MSC Circular 443 in 1986. These provided recommendations and comprehensive guidance for the security of passengers and crews. However, no legislation was produced and it was generally left to individual countries, ports or shipping companies to develop their own security provisions.

The situation changed completely in the aftermath of the terrorist attacks in the United States on 11 September 2001. Various countries, particularly the United States, concluded that it was likely that terrorists would either use ships as weapons, or to carry weapons or terrorists into a target country, or that they would attack ships to cause chaos in international trade and the international economy. A number of subsequent terrorist attacks on merchant ships have occurred, such as the attack on the Limburg off Yemen in October 2002 by a small boat containing explosives.

Ship Security

The IMO has provided the main international forum for the development of measures to meet this threat by increasing the security of ships and ports. The introduction of many of these measures was approved at a diplomatic conference held at the IMO in London in December 2002 and came into force in July 2004.

At the centre of the new security provisions were amendments to the SOLAS Convention and a security code, known as the International Ship and Port Facility Security (ISPS) Code.

This briefing highlights the main provisions of the international regulations and provides some practical guidance to ship operators about the steps they should take to implement them. It will also address some of the practical concerns and commercial implications of the rules.

ISPS Code

At the heart of the IMO ship security measures is the International Ship and Port Facility Security (ISPS) Code. This applies to port facilities serving ships on international voyages, to all passenger ships on international voyages and to all other ships over 500 GT on international voyages.

The ISPS Code was introduced by an amendment to Chapter XI of the SOLAS Convention and has two parts. Part A contains the mandatory requirements and Part B provides guidelines on how to meet them.

Although Part B of the Code is not mandatory, it does provide port facility operators, ship operators and seafarers with a comprehensive guide to the requirements of the ISPS Code. As with all such official guidance, failure to follow its provisions might be seen as a failure to exercise due diligence and Members should therefore take all reasonable steps to comply with Part B as well as Part A of the Code.

Security Assessment

The ISPS Code is intended to work on the basis that security measures are implemented in proportion to the potential risk to security, which may vary from time to time. The government of a country, or a Designated

Authority within the government, will assess the likely security threat and set the security threat level required at each of its port facilities accordingly. Updated information about security threat levels and measures will then be provided to port facilities and ships. Governments also have to provide a point of contact through which ships can get advice or assistance, or report security concerns.

Three Tier Security

The different levels advise of the extent to which a security threat is considered to be present and are used to trigger appropriate protective measures both onshore and on board ships in the port facility.

Level 1 - Low risk

This is the level of threat for which normal security measures are sufficient and is the minimum level that should be maintained at all times.

Level 2 - Medium risk

At Level 2 there is a heightened threat of a security incident. Additional protective measures are required and may have to be sustained for prolonged periods while there is an increased risk of a security incident.

Level 3 - High risk

Level 3 means that there is an exceptional threat and that a security incident is probable or imminent, although it may not be possible to identify a specific target. Further intensified protective and preparatory measures are required, but these are not intended to be sustained for significant periods of time.

As the security threat level increases, the measures taken to provide security within the port are increased appropriately from Level 1 through to Level 3.

Likewise, the underlying security threat level applied to a ship will be set by the appropriate authority of the ship's flag. The effect on a ship visiting a port is that it must implement measures that provide the required level of security for the port facility, or the level set for the ship if it is higher.

Consequently, a ship's security plan must contain measures that can be implemented for each of the three security levels - as the required security level increases, the measures taken to provide security on the ship are also increased.

Part B of the Code contains guidance about the factors that a government, or their Designated Authority, take into

account when setting a security threat level for port facilities or ships.

Company Security Officer (CSO)

Every company has to designate a Company Security Officer (CSO) whose responsibility is to ensure that Ship Security Plans are developed and approved for the ships operated by the company.

The Company Security Officer has to ensure that the Ships' Security Plans are maintained, modified if necessary, and audited. He also has to ensure that security assessments are carried out, the appropriate level of security enforced and that effective communications are established with port security officers when ships are in port.

Shipping companies already have a Designated Person, or persons, to administer and audit the ISM Code. As they will already have lines of communication in place, as well as the training and expertise to develop procedures and carry out audits, in some companies it may be appropriate to extend their area of responsibility to include security.

Ship Security Assessment (SSA)

At the centre of the measures required by the ISPS Code is the Ship Security Plan, which is specific to an individual ship and based on a security assessment of the ship.

Detailed guidelines for carrying out a security assessment of a ship are provided in Part B of the Code. The assessment should include:

- Identification of existing security measures
- Identification of key shipboard operations requiring protection
- Identification of threats to the key shipboard operations and the likelihood of them occurring
- Identification of weaknesses in the ship's infrastructure and procedures.

Ship Security Plan (SSP)

Following the security assessment a Ship Security Plan can be developed to include measures to:

- Identify the areas of the ship where access is to be restricted
- Appoint a Ship Security Officer and specify the security duties of shipboard personnel
- Prevent weapons and other dangerous devices being taken on board the ship
- Respond to a security threat or security breach and report incidents
- Interface with port security procedures
- Evacuate the ship in the event of a security threat
- Respond to government security instructions.

The actions taken to meet the above requirements will need to become more thorough as the security level under which the ship is operating is increased.

Part B of the Code provides guidelines on the measures to be taken at each of the three security threat levels, to control:

- Access to the ship
- Restricted areas on the ship
- Handling of cargo
- Delivery of stores
- The monitoring of security.

The Ship Security Plan also has to contain provisions to ensure that the crew are trained, drills are carried out, records are kept, and the procedures audited.

The plan could of course provide essential information for anyone wishing to pose a threat to the ship, so it must be protected from unauthorised access or disclosure, including disclosure to officials in port.

However there may be special circumstances in which authorised officials are allowed to look at the plan and verify that the ship security requirements have been met. To maintain security a ship should carry two versions of the plan, a confidential version and less restricted version. Only this latter version should be disclosed to port

officials, and should not contain details of passwords, codes, or the location of certain items of equipment.

The development and auditing of security plans is something that is beyond the expertise of most shipping company staff. The Company Security Officer is therefore not expected to assess and develop security plans himself, but has the responsibility of ensuring that security assessments are carried out and plans developed by competent persons or security organisations on the shipowners' behalf.

Ship Security Officer (SSO)

A Ship Security Officer is designated for each ship with the responsibility to ensure that the Ship Security Plan is properly implemented, the crew trained and drilled, and most importantly, that security awareness and vigilance are maintained.

It is up to each company to decide who to appoint as Ship Security Officer. Given the level of experience and seniority that may be required, the most appropriate choice is probably the chief officer, but the ISPS Code does not specify any particular person.

Declaration of Security (DOS)

When a ship is in port, a government may require that an agreement is reached between the ship and port authorities about the security measures to be taken at the interface between the ship and the port facility, which are the areas where people move between the ship and the shore, or where cargo is loaded. The agreement should specify who will be responsible for implementing the security measures.

This agreement takes the form of a Declaration of Security, signed by the ship's master or Ship Security Officer and a representative of the shore-side authorities.

A Declaration of Security is unlikely to be required in every case, but a prudent master and Ship Security Officer should be prepared to implement an agreement when necessary.

A Port Facility Security Officer (PFSO) or a ship can also request a Declaration of Security to be completed, for example if the ship is operating at a higher security level than the port facility.

Training and Drills

The success of any management system and procedures depends on the motivation and familiarity of those carrying them out. Shore-side staff and seafarers have not traditionally been expected to be experts in security, so proper training and drills are essential to ensure success. The Company Security Officer, Ship Security Officers and other appropriate personnel need to be given adequate training by a suitable security organisation.

Seafarers also need to be familiar with their security duties and responsibilities under the security plan and to have practice drills for different security scenarios, such as a bomb threats, attacks, and other breaches of security. According to Part B of the ISPS Code, drills should be carried out at least every three months or after certain crew changes.

Records

As with any other management system, records need to be kept for audit purposes and to show that due diligence has been exercised, as well as for inspection by authorised persons in port. The Ship Security Plan requires a number of records, including but not limited to:

- Records of training, drills and exercises
- Reports of security breaches and incidents
- Changes in the security level in operation
- A record of audits and reviews.

Records may be kept in electronic format, but in all cases must be protected from unauthorised access or disclosure.

International Ship Security Certificate

The ship's security system, equipment and plan are all subject to verification to ensure that they comply with the requirements of SOLAS and the ISPS Code. After a satisfactory initial verification, an International Ship Security Certificate will be issued. This certificate is valid

for five years after which it needs to be renewed. The certificate also requires a satisfactory intermediate verification, and any additional verification required by the ship's Flag State, to remain valid.

In some special cases the Flag State administration may issue an Interim International Ship Security Certificate, which lasts for up to 6 months, while the full certificate is being issued.

Recognised Security Organisation (RSO)

The International Ship Security Certificate is issued by the ship's Flag State, but not all governments will be able to, or want to, carry out some of the duties under the ISPS Code themselves. The government or Designated Authority can appoint a Recognised Security Organisation to carry out duties such as approving Ship Security Plans, carrying out verification surveys and issuing International Ship Security Certificates on its behalf.

The ISPS Code specifies that these Recognised Security Organisations must have the relevant expertise and knowledge in security, but should not carry out these duties if they have been involved in the related security assessment or drawing up the Ship Security Plan.

Ship's Equipment

A number of changes to ships and their equipment have been introduced to meet the latest security requirements for ships trading internationally. To provide some guidance and information to ship operators, the main features of these measures are summarised on this page.

Automatic Identification System (AIS)

An automatic identification system fitted to a ship provides shore stations and other ships with information that includes its identity, type, position, course and speed. The system must also be able to receive similar information from other ships in the vicinity.

The original intention of AIS was to increase navigational safety by providing information about a ship to shore stations and other ships in the vicinity to enable them to identify, monitor and track it. This would obviously also be a useful security measure as shore stations and defence organisations would be able to identify and monitor ships in their waters more easily.

A serious worry is that the information transmitted by a ship's AIS, including the ship's identity, course and speed, will be available to anyone with suitable receiving equipment. This would include terrorists, pirates and belligerent nations wanting to intercept and board or attack a particular ship.

Ship identification number

Every ship has a unique IMO number, which remains unchanged during the ship's life regardless of any other changes such as to the ship's name, flag or owner. Knowledge of the IMO number therefore provides a straightforward means of identifying a ship and finding out about its history.

The IMO thus makes identification easier by requiring the IMO number to be easily visible from outside the ship. It is to be permanently marked in a contrasting colour in specified places on the ship, such as on the stern, above the load line on either side, on the front of the superstructure, or on either side of the superstructure.

Ship security alert system

The concept of the security alert system is that a ship should be able to alert the company and authorities ashore by activating an alert from the bridge, or from at least one other place on the ship, if there is a security threat. When the administration of the ship's flag, or the state whose waters the ship is in or near, receives an alert they have to advise each other.

The regulations specify that no alarm should be raised on the ship itself or on any other ship.

However, the actual method of sending the alert and the method by which receipt of an alert is confirmed is not specified. The amendments to SOLAS only require that ships should be able to send an alert and that authorities ashore should be able to receive them. The response that should be taken by a Flag State or other country is not specified.

Equipment required by ISPS Code

Most ships need to be fitted with additional security equipment, such as door locks and screening equipment, to comply with the ISPS Code.

Management Systems

Changes to the ships equipment are relatively easy to understand and introduce, even if there is an obvious cost implication. When it comes to management systems, things are not always so straightforward. Some of the amendments to Chapter XI of the SOLAS Convention require the introduction of additional management systems designed to make many aspects of the ownership and operation of a ship more transparent. The main features of these requirements are summarised below. Many also have commercial implications, which are considered later.

Responsible persons

Authorised officials in countries that a ship visits may need to contact the relevant persons in the shipping company directly to request or verify information for security purposes. The ship needs to have up-to-date documentation on board to identify the Company Security Officer (see page 3) and also:

- The persons in the shipping company who appoint the crew
- The persons in the shipping company who decide the employment of the ship
- The parties to any charterparties the ship is employed under.

Continuous synopsis record (CSR)

Another measure intended to provide a complete history of the ship, and hence identify anything in its past that might present a security threat, is the Continuous Synopsis Record (CSR). This provides an on-board record of the ship's history and any changes. The information includes, but is not limited to, details such as:

- Ship's name
- IMO number
- Flag State
- Registered owner's name and address
- Classification Society
- Organisation issuing ISM certification
- Organisation issuing ship security certification.

Although it is the ship operators' responsibility to keep the information up to date, the Flag State administration actually issues the CSR. The CSR should be kept on board and made available to any authorised person for inspection, and a copy is held by the Flag State. If the ship changes flag, copies of existing CSR documents are to be retained on board and the old Flag State sends copies of its records to the new Flag State. The process is intended to prevent the history of the ship being falsified in any way.

Any changes to relevant ship's details have to be notified to the Flag State, which in turn has three months to issue a revised CSR. A potential problem with this is that a Flag State might not have the administrative capability to deliver a new CSR document to the ship within the required time, in which case the master or company will be authorised and required to amend the CSR on board. In the meantime this could lead to problems for the ship during port calls.

Control and Inspection of Ships in Port

Ships need to be able to meet security requirements at a number of different levels depending on the security threat determined to exist for the particular ship and the port being visited. These security threat levels, ranging from 1 (lowest threat) to 3 (highest threat), were described on page 2.

When a ship visits a port, the authorities of that country may require information to be provided before the ship is allowed to enter port, or to inspect the ship, to ensure that it can meet the level of security required. Appropriate records need to be kept from the last 10 ports visited.

If the ship does not have a valid International Ship Security Certificate, or there are "clear grounds" that a ship is a security threat, the authorities can deny the ship entry into

port or enforce their own security requirements and detain, restrict operations, or even expel the ship.

Part B of the ISPS Code gives some examples of "clear grounds", such as evidence of deficiencies in security equipment, evidence that the master and ship's crew are not familiar with shipboard plans, or that security exercises and drills have not been carried out. Other instances may occur if the ship is considered to present a security threat, for example, if persons who have been rescued at sea are on board the ship.

Security of People on Ships

Probably the most crucial security measures are those used in the employment and identification of ships' crew, as well as identification of other persons allowed to board a ship in port. The security measures for ships' crews are to prevent anyone who could be a security threat from becoming a member of the crew or impersonating a crew member.

Ships' security measures in port should only allow persons who do not pose a security threat, and have proper identification, to board a ship.

Pre-employment check

Under the STCW Convention ship operators are required to ensure that seafarers have the appropriate qualifications, and are also required to maintain full employment records of their sea staff.

Ship operators are also required to ensure that seafarers are medically fit, and many organisations, including P&I Clubs, strongly recommend instituting a system of suitable pre-employment medicals for this purpose. Members should consider extending this exercise of due diligence to incorporate an appropriate security check on seafarers' backgrounds before employment commences.

Master's powers

Under SOLAS, Chapter XI-I, regulation 8, ships' masters are allowed to make decisions regarding the security of the ship regardless of constraints imposed by the company, charterers or anyone else. The regulation also makes it clear that a master's first responsibility is for the safety of the ship.

Masters may deny access to persons or refuse to load cargo, if they judge it necessary in order to maintain the security of the ship. Moreover, the company is required under the ISPS Code to emphasise the master's authority and provide assistance to him if requested.

However, masters are not allowed to refuse access to a person duly authorised by a government. Although Part B of the ISPS Code encourages governments to ensure that officials are issued with appropriate identification documents, there is no internationally recognised requirement for authorised persons to carry suitable identification, such as an identification card containing a photograph, or for there to be a procedure to verify them. This could result in the bizarre situation of a master getting into trouble for refusing access to a person who turns out to be an authorised official, even if that person did not carry any reasonable identification.

Another problem relates to a master's practical ability to identify cargo posing a security threat to the ship, for example within the cargo on a 13,000 TEU container ship.

Safe manning

Safe manning levels have traditionally only related to the safe navigation of a ship. Part B of the ISPS Code advises Flag States to consider the additional workload that may result from implementation of new security measures when setting the statutory safe manning levels of ships.

Practical Advice to Ship Operators

Part B of the ISPS Code gives comprehensive guidance about the measures that ship operators and seafarers should take to make their ships secure. Practical advice on how to assess, plan and implement these measures is not given in the ISPS Code, as these are subjects about which ship operators should obtain specialist advice.

However, the following paragraphs highlight examples of the sort of measures ship operators might need to implement in three key areas of ship security - access, searches and restricted areas.

Access

At any level of security, access to the ship should be tightly controlled. Initially this means establishing the ways by which access can be gained, for example using

mooring ropes and cargo equipment, as well as by accommodation ladders, gangways and ramps.

The approved access route, usually the accommodation ladder, should be permanently manned and only persons who have a proper reason should be allowed to board. All persons boarding should be positively identified by an appropriate means of identification, such as an identity card or boarding pass including a photograph, which can be verified.

Having established controls on the authorised access routes, the unauthorised routes should be guarded. This can be achieved by closing and locking ship-side doors, removing over-side ladders, fitting guards on mooring ropes or anchor cables and ensuring that the deck and over-side areas are well lit. The deck areas need to be patrolled regularly and the patrols also need to observe the land and sea approaches to the ship. Closed circuit television cameras could also be used.

As security threat levels are increased, restrictions imposed on persons authorised to board, and the number and frequency of patrols will need to be increased appropriately.

Searches

Anyone travelling by air is used to having a routine search of their person and their baggage. Similar precautions, in liaison with the port facility, may now be appropriate for anyone boarding a ship and inspection areas may need to be set up – manned by suitably trained ship and/or port staff. The inspections should look for prohibited weapons and explosives on persons, and in carry-on luggage and baggage. Inspections will also need to be carried out on ship's stores and spare gear.

The extent of the inspections will depend on the level of security required. In addition to physical examination, equipment such as metal detecting wands, X-ray machines and explosives vapour detectors may be used.

Restricted areas

Although access to the ship is controlled, there is still a possibility that unauthorised persons may get on board, or that authorised persons such as stevedores may try to enter spaces where they are not allowed. The second line of defence on the ship is to designate restricted areas to which no one has access except authorised members of the crew.

Anyone else, such as a surveyor or Port State inspector, will need to obtain permission and should always be accompanied.

Examples of restricted areas are the bridge, machinery spaces, crew accommodation, cargo spaces and stores spaces. Fitting suitable locks, surveillance monitoring equipment and devices that detect intruders automatically, can protect these. Restricted areas should also be patrolled regularly, and guarded in times of heightened security

P&I Cover - Frequently Asked Questions

A number of questions are regularly asked about the P&I cover available for claims involving the security of ships and terrorism. The most frequently asked questions are answered below:

Does P&I cover Members' increased costs and expenses as a result of having to provide extra security precautions?

No - These are operational matters and the costs and expenses are not recoverable from P&I.

Security precautions may be required by international legalisation, such as the ISPS Code, or local rules. For example, security guards may be required in the United States on ships where not all the crew members meet visa requirements.

Members should consider increasing their commercial rates to pass on some of the burden to shippers and charterers. Consideration should also be given to incorporating suitable clauses in charterparties.

Does P&I provide cover for fines arising from a failure to comply with security regulations?

Perhaps - Members' P&I liabilities for fines are covered providing that a Member has taken reasonable steps to avoid the event giving rise to the fine. This includes taking proper steps to be aware and comply with security regulations.

National regulations, such as the 24-hour manifest rule imposed by the US Customs Services for goods being imported to the United States, may oblige the carrier to provide information about cargo being carried and describe the cargo precisely in cargo manifests and bills of lading. A failure to comply can result in fines and/or the delay or refusal by customs to permit the non-complying cargo to be discharged.

If the authorities refuse to allow cargo to be discharged, cover for a Member's resulting liabilities, costs and expenses will be considered by the Association on a case-by-case basis and any claims arising may be subject to the discretion of the Association's Directors.

Does P&I provide basic cover for terrorist incidents?

No - Claims arising from war risk type incidents, which include terrorist acts, have always been excluded from normal P&I cover. The P&I Club Directors retain a right to decide whether or not any act constitutes an act of terrorism.

Members should obtain cover for terrorism under a separate war risk policy, available from commercial war risks insurers in the marine insurance market or from a small number of mutual insurers. The risks covered by these policies should include protection and indemnity risks insurance for P&I type risks.

Does P&I provide top-up cover for terrorist incidents?

Yes - P&I Clubs in the International Group of P&I Clubs provide additional cover for war risks, including acts of terrorism, provided that a Member has suitable underlying cover provided by war risks insurers. If a war risk claim exceeds the underlying war risks market cover, P&I Clubs in the International Group of P&I Clubs provide additional cover to a Member of up to US$500 million per claim.

Because of this provision, P&I Clubs in the International Group require their Members to have separate standard hull war risks insurance for loss or damage to the ship. They also require the hull war risks insurance to be at least to the proper value of the entered ship and to contain a P&I inclusion clause, which provides cover for P&I type liabilities mentioned above.

What is a war risk area?

In a time of war or conflict, the areas where war risks apply are defined and published by the Joint War Risks Committee in the London market. In that case war risk insurers may declare the area to be an "additional premium" area, and basic war risks cover may be cancelled and reinstated at a higher rate.

Are P&I premiums increased in war risk areas?

Not usually - P&I Clubs in the International Group of P&I Clubs do not generally impose extra premiums because the primary P&I type risks are covered elsewhere and the Clubs' involvement is restricted to provision of the top-up cover described previously.

If necessary, the International Group of P&I Clubs may declare "prohibited areas", as a result of which the additional top-up cover may be terminated.