

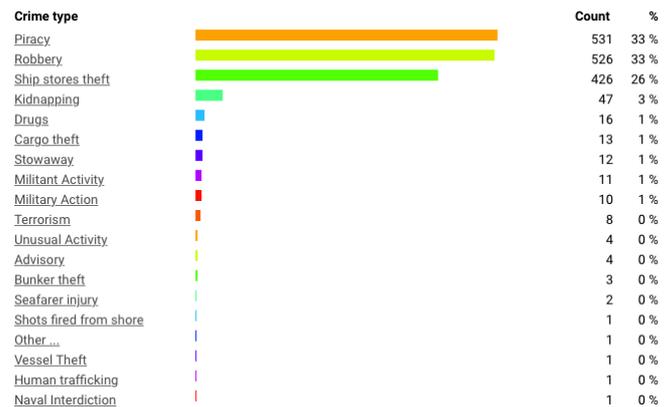
# Maritime Security: General Recommendations

## Contents

Introduction .....	1
What is piracy? .....	2
What is armed robbery? .....	2
International organisations .....	2
BMP5 .....	4
Global counter piracy guidance for companies, Masters and seafarers.....	4
Maritime global security site.....	5
Planning and preparation.....	5
General actions in the event of an attack .....	8
Insurance cover for piracy.....	9
Appendix 2 - Glossary of abbreviations .....	11

## Introduction

Piracy and maritime criminal activities continue to be a global problem. Even with measures in place to combat issues, there still exists a significant risk of attack to vessels transiting certain geographical areas.



*Reported maritime criminal activity worldwide from 2013 to 2016, information taken from CSO alliance.*

### Disclaimer

The purpose of this publication is to provide information which is additional to that available to the maritime industry from regulatory, advisory, and consultative organisations.

Whilst care is taken to ensure the accuracy of any information made available (whether orally or in writing and whether in the nature of guidance, advice, or direction) no warranty of accuracy is given and users of the information contained herein are expected to satisfy themselves that it is relevant and suitable for the purposes to which it is applied or intended to be applied. No responsibility is accepted by North or by any person, firm, corporation or organisation who or which has been in any way concerned with the furnishing of data, the development, compilation or publication thereof, for the accuracy of any information or advice given herein or for any omission herefrom, or for any consequences whatsoever resulting directly or indirectly from, reliance upon or adoption of guidance contained herein.

As can be seen from the above statistics, piracy and armed robbery remain the main risk to maritime security.

This briefing provides information on the prominent international organisations involved in combatting maritime crime. It also includes some of the suggested steps that could be adopted to protect the ship and crew whilst operating in, or transiting an area of high security risk.

This briefing should be read in conjunction with the regional briefings which can be read here:

### LP-briefings/ships

*Maritime Security – Western Indian Ocean*

*Maritime Security – Gulf of Guinea*

# Maritime Security – General Recommendations

## Maritime Security – South East Asia

For a glossary of the abbreviations used in this briefing see appendix 2 [here](#).

## What is piracy?

UNCLOS, Article 101 contains the following definitions for Maritime Piracy:

Piracy consists of any of the following acts:

- (a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
  - (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
  - (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
- (b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
- (c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

## What is armed robbery?

The IMO define armed robbery in their “Code of Practice for the Investigation of the Crimes of Piracy and Armed Robbery against Ships,” as any of the following acts:

- a) any illegal act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or against persons or property on board such a ship, within a State's internal waters, archipelagic waters and territorial sea;
- b) any act of inciting or of intentionally facilitating an act described above.

## International organisations

This section summarises the main organisations involved in the global protection of commercial shipping. It also includes recommended information sources for maritime security. For region specific organisations covering the Western Indian Ocean, Gulf of Guinea, or South East Asia, please see the relevant Loss Prevention Briefing for that geographical area.

### The International Maritime Organisation, (IMO)

The IMO has been working to combat piracy since 1983, when its assembly passed a resolution calling on governments to take urgent measures to prevent and suppress acts of piracy in or adjacent to their waters.

In order to provide accurate and up-to-date statistics on the nature and extent of the problem, the IMO also called on its members and non-governmental organisations, such as ICC/IMB, BIMCO and ICS, to submit details of all attacks of which they become aware.

The IMO also operates a Piracy and Armed Robbery module found in its Global Integrated Shipping Information System. Here information about acts of piracy and armed robbery are available to the public after registration.

<https://gisis.imo.org/Public/Default.aspx/>

Following a joint meeting with industry representatives in October 2008, the IMO called for sustained coordination between all naval forces operating in the area and for clear rules of engagement that would enable military assets to intervene effectively to protect shipping.

The IMO has published much guidance to assist in the reduction of cases of armed robbery and piracy. This guidance has been issued for governments, ship owners, ship operators, and ship's crews.

For further information on IMO guidance please use the below link:

<http://www.imo.org/en/OurWork/Security/PiracyArmedRobbery/Pages/Default.aspx>

# Maritime Security – General Recommendations

## International Maritime Bureau (IMB)

The IMB is a specialised division of the International Chamber Of Commerce (ICC). It is a non-profit making organisation, established in 1981 to act as a focal point in the fight against all types of maritime crime and malpractice.

In 1992 the IMB PRC, commenced a free 24 hour service to commercial shipping that allows them to report any incidents of piracy, armed robbery or stowaways.

The PRC is a worldwide single point of contact for ships that have been attacked, or have been approached by a suspected attacker. Information received by PRC is relayed to local law enforcement who in turn can deliver assistance.

The ICC offer many facilities on their website including advice to vessels Masters and a live piracy map.

Contact details for the PRC are as follows:

<https://www.icc-ccs.org/piracy-reporting-centre>

The 24 hour hotline details are:

Email: [piracy@icc-ccs.org](mailto:piracy@icc-ccs.org)

Tel: +603 2031 0014

Fax: +603 2078 5769

## INTERPOL

INTERPOL is an international police organisation with 190 member countries. Its aim is to allow police forces around the world to collaborate in combating international crime.

INTERPOL operates a Maritime Piracy Task Force which focuses its efforts in the following areas:

- Improving evidence Quality – This is an advisor and training initiative that is extended to member countries to show how evidence is gathered, analysed and maintained in piracy cases.
- Facilitating Data Exchange – This function assists in information sharing between nations involved in piracy cases. They operate a secure global police communications system, known as I-24/7, and our system of Notices are key to the sharing of data and the detention of suspected pirates.

- Building regional capabilities – Helping regional police forces in the fight against piracy and armed robbery with specialised training and equipment.

## United Kingdom Hydrographic Office – SRIM

The UKHO has produced a series of security charts that at the time of publishing this briefing are as follows:

- Chart Q6099 - Red Sea, Gulf of Aden and Arabian Sea
- Chart Q6110 - Mediterranean Sea
- Chart Q6111 - Persian Gulf and Arabian Sea
- Chart Q6112 - Karachi to Hong Kong
- Chart Q6113 - Andaman Islands to Torres Strait including Indonesia
- Chart Q6114 - West Africa including Gulf Of Guinea

It is strongly advised that vessels operating in the above outlined areas carry and update these charts. The charts clearly outline the voluntary reporting areas for the regions as well as showing the means of communication to security support facilities.

## Joint War Committee

The Joint War Committee of the International Underwriting Association (IUA) and Lloyd's Market Association (LMA), offers relevant security information on their website. This includes information on the UKTMO, an update on the current situation in high risk ports, bulletins and circulars, and advice on best practise for operating in a known high risk area.

More information can be obtained by subscribing to the Joint War Committee Members area at:

<http://www.lmalloyds.com/lma/jointwar>

## CSO Alliance

CSO Alliance is an online security community hub that aims to open channels of communication for company security officers to discuss issues and share information.

It includes secure chat areas, maritime security reports, the latest security news and a live piracy map.

# Maritime Security – General Recommendations

It can be of great assistance in compiling a voyage risk assessment.

North supports the concept of information sharing in security related issues. As such we believe membership to the CSO Alliance site will offer real benefits to CSOs employed by North members.

Membership fees will be reduced by 20% for North members by CSOA and for the first year North will subsidise a further 40% of the fee for one CSO per member.

For more information on CSOA and membership see below:

<http://www.nepia.com/our-services/loss-prevention/signals-online/cyber-risks/cso-alliance-september-2016/cso-alliance/>

The CSOA site can be accessed here:

<http://www.csoalliance.com/>

## Maritime threats and incidents

Gray Page in partnership with North operates the Maritime Threats and Incidents interactive risk map. It provides background information, analysis and assessments relating to the commercial risks and physical threats ('enduring risks') faced by the shipping industry and seafarers, around the world.

The risk map can be located on the North site here:

<http://www.nepia.com/maritime-alerts/>

This free service is another information source that can be referenced during voyage risk assessment.



North's MTI page

## BMP5

Best Management Practice 5 – To deter piracy and enhance maritime security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea.

BMP5 contains good advice on general vessel hardening, and is another source of reference for vessel preparations when conducting voyage risk assessments for any area.

BMP5 can be found at the following link:

<http://www.mschoa.org/docs/default-source/public-documents/bmp5.pdf?sfvrsn=2>

## Global counter piracy guidance for companies, Masters and seafarers

This guidance document consists of general advice and recommendations for the CSO, Master and crews to prevent attacks along with guidance on conducting voyage risk assessments and planning.

As well as piracy and armed robbery, the guidance covers terrorism and cyber threats.

Global counter piracy guidance for companies, Masters and seafarers can be found at the following link:

# Maritime Security – General Recommendations

<https://www.ocimf.org/media/91171/Global-Counter-Piracy-Guidance-For-Companies-Masters-and-Seafarers.pdf>

## Maritime global security site

This is an industry website which is supported by a number of shipping industry associations, including the International Group of P&I clubs. It provides guidance and information for companies and mariners seeking on a wide range of Maritime Security Issues.

The maritime global security website can be found at the following link:

<https://www.maritimeglobalsecurity.org/>

## Planning and preparation

### Voyage Risk Assessment

The CSO and the vessel's Master have combined responsibility to produce a voyage risk assessment. The procedure for this should be outlined in the vessels SMS. The risk assessment should include:

- Highlighting areas of increased threat to the vessel.
- Identify the high risk areas for that region.
- Understand the methods often used by pirates in these areas, and access vulnerable areas where pirates could board.
- The ships own characteristics including handling, freeboard, speed, general arrangement.
- Military or official organisation cooperation and reporting requirements.
- Existing guidelines and information sources.
- Ship and company procedures, communication and chain of command.

Masters and CSOs should assess the likelihood and consequences of piracy attacks based on the latest available information. The outcome of this risk assessment should identify measures for prevention, mitigation and recovery. This will mean combining statutory requirements with supplementary measures to combat piracy. It is

important that risk assessments are ship and voyage specific.

Operators should implement appropriate measures to meet the threat of piracy by adopting IMO and other industry recommended practices suitable for the circumstances of the voyage and ship type. Prior to entering the HRA the Master should ensure that all appropriate BMP measures are in place and crew members should be thoroughly briefed and participate in security drills.

Operators and Masters should review the Ship Security Assessment and implementation of the Ship Security Plan, as required by the International Ship and Port Facility Code to counter the piracy threat.

A policy defining the use of the vessel's AIS with regard to transmitting vessel data should be established.



## General vessel hardening

Vessels operating and transiting areas with an increased risk of attack should have guidance on general vessel hardening within their company's management system. It may be based on the above outlined voyage risk assessment requirements.

A vessel's defence should be layered. This is to ensure any partial failures in the defence system do not leave the vessel vulnerable to attack. An example of this is:

<u>1<sup>st</sup> Defence Layer</u>	<u>2<sup>nd</sup> Defence Layer</u>	<u>3<sup>rd</sup> Defence Layer</u>
Maintain a good look out	Lock down all exterior doors	Lock down all interior doors.

Advice on vessel hardening from other official sources includes measures such as:

# Maritime Security – General Recommendations

- Compliance with the International Rules for Prevention of Collision at Sea at all times; navigation lights should not be turned off at night. Masters should follow any guidance given by the Flag State.
- Whenever possible, avoid areas where there exists an increased risk of attack, or select a route away from areas of high attack frequency.
- Proceed at maximum speed with critical machinery fully operational.
- Taking into account manning levels, ensure that ship routines are adjusted sufficiently in advance to ensure well-rested and well-briefed crew are on watch and sufficient watch-keepers are available.
- Keep a good lookout for suspicious craft, especially from astern. Most attacks have occurred from the quarters.
- Consider shorter watch rotation to maintain crew alertness.
- Use light, alarm bells and crew activity to alert potential pirates that they have been detected.
- Follow the procedures laid down in the Ship Security Plan and identify a safe area within the vessel (locked down accommodation / engine room).
- Endeavour to establish radio silence (VHF and UHF handsets), except in case of emergency or for navigational reasons.
- No work should occur outside the accommodation unless essential.
- Fire pumps should be set running and hoses pressurised with water spray discharged overboard in highest risk quarters.
- Endeavour to operate at least two generators and at least two steering motors.
- Machinery spaces should be continuously manned.
- Check all ladders and outboard equipment are stowed or up on deck. If the ship has a comparatively low freeboard, consider the possibility of extending the width of the gunwales to prevent grappling hooks from gaining hold.
- Consider the use of dummies at the rails to simulate additional lookouts.

- However, if ship design creates lookout black spots and the security assessment identifies this risk then it may have to be covered by manpower.

For vessels consistently engaged in HRAs, owners may wish to make permanent alterations to the vessel, such as adding additional lockable barriers. Some ship operators employ a private security company for the transit, as discussed later in this briefing.

The following additional measures are commercially available options to increase a vessel's self-protection. Their effectiveness and reliability cannot be confirmed and their use remains the decision for the individual ship owners/operators:

- Barbed wire/physical barriers around stern / lowest points of access.
- The use of physical barriers to protect the bridge watchkeepers, (Kevlar / sandbags or equivalent).
- Electrified fencing (not recommended for oil tankers or gas carriers).
- High intensity lighting.
- LRAD (long range acoustic device).
- Consider using night vision optics.
- Additional barriers on the bridge deck as this is often a focus for attackers.

# Maritime Security – General Recommendations



*Image courtesy of CSO Alliance*

## Safe muster points

A safe muster point is a pre designated area that provides protection for the crew. If under attack it acts as a short term safe zone for those not required on the bridge, or in the engine control room, can muster as a short term safe zone when under attack.

## Vessel citadels

As opposed to a safe muster point, a citadel is an area that is purpose built and is constructed to resist forced entry. Citadels should be equipped with means of communication to ashore.

## Unarmed private maritime security contractors

The use of private security firms is often considered. However, their employment is a matter for the individual ship operator following a risk assessment.

The use of experienced and competent unarmed private maritime security contractors can be a valuable addition to best management practice.

## Armed private maritime security contractors

The decision to use armed maritime security providers on board merchant vessels is a matter for individual ship operators to decide following their own voyage risk assessment. It is also subject to the approval of respective Flag States. If Armed Maritime Security Providers are to be used they should be as an additional layer of protection and not as an alternative to the vessels own deterrents under best management practice.

It is important to be aware that certain countries and territories will not allow the entry of armed security contractors. Also, some Flag States restrict the use of armed contractors. As such, members are urged to investigate the legal position of continuing with armed contractors.

The IMO has produced guidance in the form of MSC Circular MSC.1/Circ.1405 for ship operators and masters on the use of Armed Maritime Security Providers in the High Risk Area:

[IMO MSC.1/Circ.1405/Rev.2](#)



*Image courtesy of CSO Alliance*

# Maritime Security – General Recommendations

## GUARDCON

BIMCO have developed an agreement for the hire of private maritime security guards, either armed or unarmed.

GUARDCON was developed to provide a clearly worded standard contract on which the industry can conclude their agreements for the use of security services on board.

It addresses the standards to which the contractor must conform in terms of:

- providing adequate insurance to cover their liabilities and contractual indemnities (which Members should verify);
- having in place the necessary permits and licences to allow them to lawfully transport and carry weapons
- liability and indemnity provisions based on knock for knock principles; and
- The Master maintains responsibility for the safe navigation and overall command of the vessel.

It is important to note that there are a number of companies offering services of private security, some more reputable and reliable than others. In order to assist ship owners BIMCO has reviewed and reinforced its guidance regarding Clause 10 of GUARDCON in relation to the use and carriage of validated firearms. In particular ship owners should ensure their appointed private marine security contractors have the required End User Certificates (EUC), officially authorised by the competent government agency in the exporting country. These EUCs should then be verified by a vessel's Flag State before issuing a letter of authority.

For more information on the use of GUARDCON please contact:

[PiracyContractReviewTeam@nepia.com](mailto:PiracyContractReviewTeam@nepia.com)

## Piracy clauses for charter parties

Intertanko has published standard clauses for both time and voyage charter parties.

BIMCO has published three piracy clauses for time charter parties, single voyage charter parties and consecutive voyage charter parties/contracts of affreightment.

The piracy clause for time charters was revised in response to industry comments that the responsibilities and liabilities of the parties, in the event of the seizure of a vessel by pirates, were perceived as being imbalanced. Two new clauses provide contractual solutions for short term spot fixtures where the cost and risk remain with owners, and also for longer term consecutive voyages and COAs where risk and cost is shared between owners and charterers.

A copy of clauses can be downloaded from the member area of BIMCO's website:

[www.bimco.org](http://www.bimco.org)

If considering the use of any of these clauses for new fixtures Members with FD&D cover should first contact a member of North's FD&D department to discuss the details of their situation.

## General actions in the event of an attack

### Approach stage

- Immediately increase to maximum speed and steer a straight course
- Follow the prepared contingency plan.
- Activate the Emergency Communication Plan; make calls to the appropriate centres for the region as established in the voyage risk assessment.
- Activate the Ship Security Alert System (SSAS), which will alert the Company Security Officer.
- If the Master has exercised his right to turn off the Automatic Identification System (AIS) during transit of the piracy area, this should be turned on once the ship comes under pirate attack.
- Sound emergency alarm and make a PA announcement 'Pirate attack'.
- Make a 'Mayday' call on VHF Ch 16 and any appropriate channels for military vessels in the area.

# Maritime Security – General Recommendations

- Send a distress message via the DSC (Digital Selective Calling), system and Inmarsat-C as applicable.
- Muster all crew in a designated safe muster area or citadel if constructed.
- Where possible, alter course away from the approaching skiffs, and/or mother ships. When sea conditions allow, consider altering course to increase an approaching skiff(s) exposure to wind/waves.
- Activate water spray and other appropriate self-defensive measures.
- Ensure that all external doors and, where possible, internal public rooms and cabins, are fully secured.
- In addition to the emergency alarms and announcements made for the benefit of the vessels crew, sound the ships whistle / foghorn continuously to demonstrate to any potential attacker that the ship is aware of the attack and is reacting to it.
- The safety of crew, ship, cargo and environment should be of paramount importance to the master.
- If the bridge and engine room are to be evacuated, then the main engine should be stopped, all way taken off if possible and the ship navigated clear of other ships.
- The crew should be instructed not to confront the pirates at any time. They should remain calm and co-operate fully with the pirates.
- Try to ensure all crew, other than the bridge team, stay together in one location.
- If in a locked down safe area, ensure internal protection/cover is available in case the pirates attempt to force entry. Keep clear of entry points/doors and portholes/windows – do not resist entry.
- It is quite possible that the pirates who hijacked the ship will not stay and guard the ship while at anchor.
- Guards will probably rotate, it is therefore important to be friendly and cooperative to all.
- As far as possible regular meal patterns, personnel hygiene and regular exercise should be maintained to remain alert, fit and calm under stressful conditions.
- In the Gulf of Aden some of the pirates are known to use the stimulant drug "khat" (spellings vary). This may make initial attempts at cooperation difficult if the pirate is in a drugged, euphoric state.

## Attack stage

- Reconfirm that all ships personnel are in a position of safety. The crew should be thoroughly briefed as to what is expected of them in the unfortunate event of being hijacked.
- As the pirates close on the vessel, Masters should commence small alterations of helm whilst maintaining speed to deter skiffs from lying alongside the vessel in preparation for a boarding attempt. These manoeuvres will create additional wash to impede the operation of the skiffs.
- Substantial amounts of helm are not recommended, as these are likely to significantly reduce a vessel's speed.
- Before pirates gain access to the bridge the crew should inform the relevant regional reporting / security centre. Ensure that the SSAS has been activated, and ensure that AIS is switched on.
- The Master will have to ensure that any tension on board is diffused; this could be done by cooperating fully with the hijackers and offering no resistance.

## Insurance cover for piracy

The International Group of P&I Clubs (IG) has produced a FAQ document to provide general clarification and guidance on a number of matters concerning insurance cover issues arising out of piracy incidents:

<http://www.igpandi.org/article/faqs>

Topics covered include;

- The definition of piracy
- An overview of the scope of cover provided by P&I, H&M, and war risks insurance.
- The use of guards.

# Maritime Security – General Recommendations

- Best Management Practices (BMP).
- General average.

Ransom payments may be funded by K&R (Kidnap and Ransom) insurers if this cover is in place it may also be covered by war or property insurers (H&M/Cargo).

# Maritime Security – General Recommendations

## Appendix 2 - Glossary of abbreviations

AIS:	Automatic Identification System
BMP 4:	Best Management Practise 4 <sup>th</sup> Edition
CSO:	Company Security Officer
CSOA:	CSO Alliance
HRA:	High Risk Area
IMB:	International Maritime Bureau
IMB PRC:	International Maritime Bureau Piracy Reporting Centre
IMO:	International Maritime Organisation
INTERPOL:	International Criminal Police Organization
ISPS:	International Ship and Port Facility Security Code
SRIM:	Security Related Information to Mariners
SSAS:	Ships Security Alert System
UKHO:	United Kingdom Hydrographic Office
UNCLOS:	United Nations Convention on the Law of the Sea
VRA:	Voluntary Reporting Area