

Anti Piracy Measures

Security Hazard Assessment

To all intensive purposes the process for a SHA is exactly the same as the JHA. Generally the process is as follows:

1. Outline the sequence of events;
2. Identify the Hazards as applicable to each event; and
3. Apply the risk control hierarchy to identify actions to manage the hazards



SHAs can be easily underutilised especially if using generic types. Generic SHAs are good starting point; however, the information in them is not exhaustive so it must be updated and checked for applicably in relation world and local events; and the availability of updated security advisories etcetera.

Another way a SHA is commonly misused is because the output is either meaningless or not implemented – a SHA is actually a construct. In application the construct of a JHA should provide you a set of work

instructions detailing when someone, a team or Department will take an action(s) at a concise point in time or at a certain point in the voyage. JHAs must be implemented properly and entirely, and the SSO should ensure each instruction has been appropriately carried out.

Based on the experience of the Author and notwithstanding the Security Risk Assessment below are number of security practices that can be applied while in Port or at Anchor; prior to and underway.

Security Best Practice

Action by Ships Masters In Port and at Anchor

Masters should carry out a full risk assessment before entering and while in Port or at Anchor. There are a number of things a Master can do to identify security risks:

1. Check high risk areas with authorities such as PI Clubs, Lloyd's website and IMB Piracy Reporting Centre; and
2. Maintain situational awareness of world events and ongoing threats.

Once identified the hierarchy of control should be applied.

When at Port, the Master must consider all operational and potential security impacts including piracy and armed robbery when deciding how many gangways are rigged. This decision should consider the security level; the allocation of resources and staff;

and additional security staff to ensure the smooth operation and secure movement of personnel. Other considerations for identified hazards are:

1. Limit the number of access points and strictly enforce access control procedures.
2. Keep a proper gangway watch as per ISPS code requirements.
3. Ensure there is good communication between the gangway and the OOW by radio and with the bridge by radio or telephone.
4. Adequate provisions should be made to ensure that the gangway watch is properly relieved when necessary for meals and regular breaks for refreshment or to use the toilet.
5. Checks ID of all visitors, log them on and off the vessel.
6. Check credentials of agent's port state control inspectors etc.
7. Implement stringent identification procedures to include conducting 100 percent "hands on" checks of security badges for all personnel, if badges are required.
8. Remind ships personnel to properly display badges, if applicable, and enforce visibility.
9. Escort all visitors entering and departing. Do not allow visitor's passage through the ship unescorted.
10. Call a duty officer and have them escorted to where they want to go.
11. Require two forms of photo identification for all visitors. i.e. Company ID plus National ID passport or driving licence.
12. The visitor's official ID should be exchanged for the visitors pass. Spare visitor's passes must be carefully controlled.
13. Missing or lost passes should be reported to the SSO as soon as the shortfall becomes apparent.
14. All visitors' passes must be accounted for and deposited with the Master or SSO on the vessel departure.
15. Validate vendor lists of all routine emergency deliveries and repair services.
16. Make use of the ships security plan to assess entry points and sensitive areas. Review the security assessment and plan to see if it is adequate with respect to piracy and attack by armed robbers at sea.
17. Carry out security patrols around the ships decks observing any movements or suspicious activity around the vessel both outboard and quay side.
18. Carry out regular checks on the forecastle or mooring deck and other deck areas for any evidence of unauthorised access.
19. Consider possible unauthorised access points the following areas should be included:
 - a) Anchor Chain;
 - b) Mooring Lines;
 - c) Embarkation Ladders;
 - d) Tyre Fenders;
 - e) Gangways; and
 - f) Another vessel alongside.
20. Carry out thorough checks to ensure that doors and access points and hatches that are open are manned by a responsible person from the department conducting the operation.
21. Ensure all levels of personnel are informed via briefings, email, voice mail and signage of any changes in threat conditions and protective measures.

22. Encourage personnel to be alert and immediately report any situation that may constitute a threat or suspicious activity.
23. Encourage personnel to take notice and report suspicious situations or persons that look out of place, i.e. strangers loitering or hanging around the vessel with no particular purpose.
24. Post emergency telephone numbers for police, fire, and rescue.
25. Encourage personnel to memorize important numbers.
26. Encourage personnel to avoid routines, vary times and routes, pre-plan, and keep a low profile, especially in ports or areas of high threat.
27. Encourage personnel to keep their department heads and supervisors apprised of their whereabouts.
28. Increase the number of visible security personnel wherever possible. Increase foot and roving security patrols varying in size, timing and routes.
29. Implement random security personnel shift changes.
30. Review current contingency plans and if not already in place, develop and implement procedures for acting in response to a threat, alert notification procedures, evasive action, procedures, attack response procedures, lockdown procedures, hostage and barricade procedures, passive resistance procedures.

When the aforementioned plans and procedures have been implemented, conduct internal training exercises to ensure

the objectives can be implemented. The following steps should also be considered:

1. Coordinate and establish partnerships with local authorities, agents, other shipping companies and ships Masters to develop intelligence and information sharing relationships.
2. Place personnel on standby for contingency planning.
3. Crew going ashore should be logged on and off and a T board maintained with status updated.
4. Crew members returning from ashore should not be allowed to bring visitors on board the vessel in any circumstances.
5. Family members should not be allowed on board unless the crew member was thoroughly vetted and only with the express permission of the Master.
6. Carry out random searches of bags.
7. Prohibit photography on the vessel and beware of mobile telephones that may be used to take sensitive photos.
8. Use a ships conference room for reception and meetings and not the Bridge or the Master's cabin.
9. Have a crew member present at all times when service engineers or contractors from ashore are working on board the vessel.
10. Check crew credentials especially if newly joining from third world agencies.
11. Ensure that they have been properly vetted and if possible check their documents on line through their national maritime administration.
12. If there is any doubt regarding the quality of the Crewing or manning

agency or their screening procedures then consideration should be given to restricting access to those crew members to non sensitive areas.

13. Sleepers are a common ploy by organised gangs of pirates.
14. A sleeper could be a local crew member passing information and photos back via mobile telephone then assisting in an attack by lowering boarding ladders ropes etc.
15. The control and identification of stevedores is the responsibility of the terminal operator, however this does not preclude security checks on stevedores boarding the ship.
16. While stevedores are working on board they should remain in their designated work area. They are not allowed unrestricted access around the ship. If found unescorted they should be challenged and escorted back to their designated work area.
17. Check the papers of local security personnel.
18. Take pictures of unknown visitors Restrict access to the bridge and secure areas to senior officers.
19. Keep manifest sailing plans and company instructions under lock and key. Privileged information should be confined to senior officers i.e. Master C/O and C/E.
20. The OOW/SSO should maintain and a key register and control the issue of all keys that are not crews cabin keys. All keys should be accounted for at all times.
21. Illuminate decks and over the side, especially bow and stern.
22. If there is any doubt the fact should be reported to the SSO or Master.

The Master is responsible for the control of the Master keys. Master keys should only be used in an emergency or exceptional circumstances or when key has gone missing and cannot be accounted for. Doors and access will normally be controlled through the key board and register. Avoid anchoring overnight in high risk areas if at all possible remain at sea well off the coast until daylight on the day of berthing. Keep chain washers in hawse pipes running while at anchor. The anchor chain is a favourite means of access for the opportunist robber and local pirate.

I know from personal experience that if I could not make the fairway buoy at the entrance of the Bonnie River in Nigeria by 15:00 hrs I would head 40 nautical miles out to sea and steam up and down until daybreak.

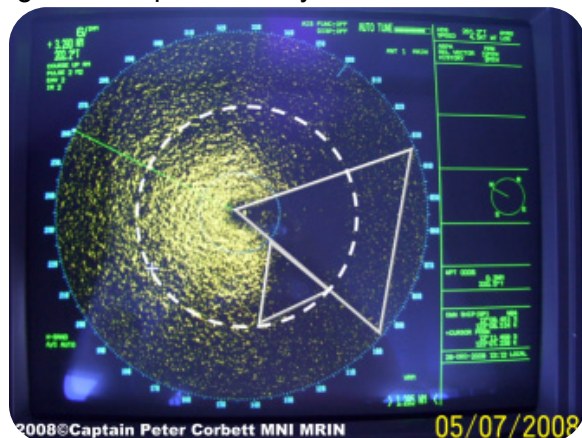
Prior to Sailing

The containment of the ships business and cargo must be considered. For information hazards you can do the following:

1. Minimise unnecessary promulgation of ships orders sailing plan etc. These should be limited to the Master and Chief Officer, Chief Engineer Prepare an additional passage plan that can be easily switched to on sailing.
2. Allow four to six hours in the voyage plan time scale in order to action a change in sailing plan.
3. When preparing appraising and reviewing a sailing plan due consideration should be given to known problem areas and every effort should be made to maximise the sea room between the vessels proposed passage and these areas.

4. Carry out a comprehensive search for stowaways prior to departure.

Stowaways like sleepers are often used by the more organised crime syndicates. Apart from the obvious threat from a security perspective finding a stowaway on board after the vessel has departed opens up a myriad of other problems for the ships Master and the company. It is by far better to find a stowaway at the earliest opportunity. On finding a stowaway search the area they were hiding or documents cameras mobile telephones. Search their persons and confiscate documents and mobile phones. If possible photograph the stowaway and keep them secure at all times, inform the company and the shipping agents and port security.

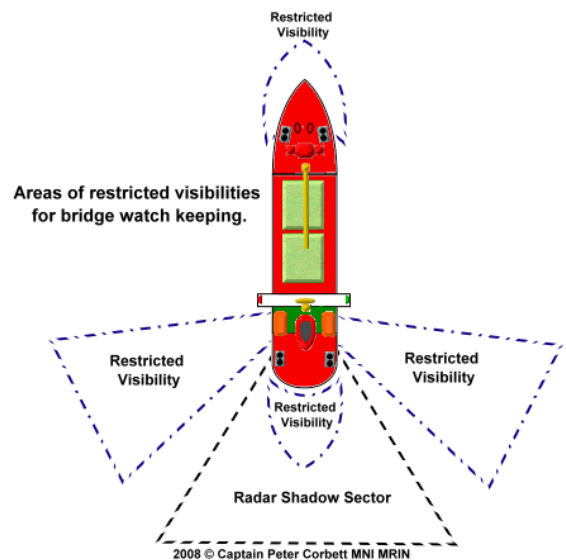


Vessel Under Way

Most Pirate attacks happen at night. Try to transit high risk areas during daylight hours. Maintain full speed safety permitting. When transiting narrow waterways and maritime bottle necks that are divided by two or more territorial jurisdiction efforts should be made to stay in or as near as possible in the

territorial waters of the nation that has the most control and can offer the best security.

Radar Shadow Sectors are vulnerable spots used by pirates to approach a ship. Ensure that the OOW and watchmen are aware of the blank and shadow sectors of the ships radar and make sure these are monitored visually. There should be a diagram of shadow sectors on the bridge. Ensure that there is diagram clearly visible on the bridge for the OOW and watch keeper illustrating both radar shadow sectors and visual blind spots.



Rig fire hoses and prepare monitors to further advertise ships awareness.

Although a ship's Master can not rely or expect assistance from another unarmed merchant if he comes under attack by pirates. There is some comfort and a small degree in safety in numbers. In as much as the more eyes the better and busy sea lanes tend to be better policed. There is also an advantage of shared intelligence through forewarning or if you are the unfortunate enough to be victim the relaying

and updating of your position and plight to the authorities. When transiting in a busy sea way the most important thing for the Master to ensure is that you make it absolutely clear to a pirate vessel that the ship is fully prepared alert to the risk and keeping a vigilant watch.

A pirate attack is an ambush and relies on surprise mobility and shock. If you look as if you are alert the chances are that they will look to the other vessels for one that looks like an easier target Master should consider making use of services such escorted convoys where available and which are in operation through trouble spots. In particular the UN corridor through the Gulf of Aden always maintain the maximum deck lighting while underway through trouble spots subject to navigation requirements. Boarding ladders pilot ladders and any portable access equipment should be removed and stowed in a locked compartment for the duration of the passage through a high risk area such as the Malacca Straights. Before voyaging through high risk areas you should maintain security patrols checking for signs of unauthorised access; check all secured spaces and doors are locked from the inside; and, ensure security seals are not broken. The following actions can also be taken:

1. Escape hatches should be secured from the inside with quick release mechanism that can be easily released in an emergency.
2. Seal access to high risk areas and especially at night keep hawse pipes sealed and gangways hoisted and with windows and doors locked with deadlights and scuttles shut and secured.
3. Ensure security grills are in places such as skylights, ventilation trunking and escape hatches. Maintain deck patrols while alongside and at sea, and ensure patrols carry good radio communications.
4. Make good use of close circuit television if fitted and operational Ensure lock down and citadel procedures are in place and have been assessed.
5. Several scenarios should be available and changed at random.
6. Hold a security meeting as soon as possible after departure to ensure the crew are aware of the emergency lock down procedures in force for the period.
7. Hold an anti piracy drill as soon as possible after every departure to ensure all crew members are conversant with anti piracy measures and procedures in place in place.
8. Hold a security meeting prior to arriving in port to ensure that all the crew are aware of the dangers and their responsibilities both to their duties on board the vessel and their personal responsibility not to discuss the ships business or movements while ashore.
9. Ensure that there are procedures for alert signals so crew know when situation is developing when to lock down when to take avoiding action and when boarders are on board.

All the crew should be briefed not to act aggressively once the vessel has been boarded. Once pirates are on board there is little the crew can offer other than passive

resistance. Senior staff should be fully trained in techniques for dealing with boarders and complying with their requirements and of the need to maintain control of the safe navigation of the ship to avoid collision grounding and other disasters. Pirates in some areas like the South China Sea and the Gulf of Aden are highly organised with substantial financial backing in addition to fast craft, heavy weapons, mother ships with the latest navigation and tracking devices. It is therefore reasonable to assume that they are using are also using AIS not only to locate targets but also to send misleading information. If encountering a pirate mother ship or suspected mother ship send a full report immediately to the IMB Piracy Reporting Centre and include the following information:

1. Your ships name, position, details, course, speed, type of vessel and cargo.
2. A general description of the suspected mother ship including name, colour of hull and superstructure, distinctive markings, approximate length, construction, type of vessel.
3. The mother vessel position course and speed.
4. Take photographs if possible
5. The number of people on board the mother vessel
6. Whether any weapons were observed on board and if possible what type.
7. Are there any skiffs on board, towed or alongside if so how many and number of engines
8. If possible take an ECDIS screen shot
9. Note if an AIS signal is broadcast.

10. Has the vessel changed course or speed to intercept or shadow yours or another vessel?

Remember:

