Security Risk Assessment for Port Facility in Compliance with ISPS Code

By
Captain Lee Ghim Teck, Malaysian Maritime Academy
lee_ghimteck@alam.edu.my
and
Dr. Muhammad Zaly Shah B Muhammad Hussein, University Technology Malaysia

on
17th & 18th April 2012
Kuala Lumpur, Malaysia

Abstract

Being the most critical interface in managing the supply chain between the local manufacturers and over sea consumer, port facilities around the world are constantly faced with various challenges in both commercial as well as in operational terms. For these challenges, port facilities need to ensure that they are fully prepared at all time in cases of unforeseen circumstances so the first, they can prevent it from occurring, second, they could allocate sufficient resources in response to such occurrences and third, in case of after event, the resources available could react in organized manner to prevent the situation from escalating to uncontrollable level.

In security risk, the main variation from safety risk is the intent. Safety generally result from internal failure to ensure preventive measures are being observed to eliminate or isolate the hazards and the occurrences are generally unintentional, whereas in security, the introduction or reactivation of hazards are done with specific objective and it is generally an intentional or planned activities. With that in mind, a systematic risk assessment approach must be put in place to ensure all possible threats are identified and appropriate security barriers are effectively in place so that any attempt to cause undesired event could be detect and deter.

This paper will be looking into various aspect that need to be taken into consideration in carryout the security risk assessment including the methodology use at the moment in carryout the risk assessment and follow-up management of the identified risks.

Keywords: Security, risk assessment, prevention, response, consequences management.
Introduction

Ports being the critical interface between the ships plying the world ocean shipping, and its 95% world seaborne trade and linking the shore logistics element of the supply chain completing the total cycle of supply and demand. At time the present of the port in specific area or location, provide another indirect economical income for the local community as well as creation of new and vibrant township. Depending on the nature of the cargo and available facilities in the port, it has to cater for varying activities and movements at all time and on 24/7 alertness. In today ever challenging demands and uncertain economic environment, port competitiveness will generally depending on the speed and efficiency of the services provided to secure the clients confidence in term of reliability and capability with safety and security in mind.

In the aftermath of the 11 September incident, the maritime community witnesses the implementation of a new security regime that involved both the ships and port facilities around the world. This new security regime is the International Ship and Port Facility Security Code or better known as the ISPS Code. It is the first time, the International Maritime Organization (IMO), which is an affiliation of the United Nation agency looking after maritime affair and head quarter in London, UK.

The Code came into force on 1 July 2004 and it applies to all vessels of 500 GT (Gross tonnage) and more trading on international voyage, as well as to all port facilities serving the above mentioned categories of vessel. For ease of implementation, the Code was incorporated into the International Convention of Safety of Life at Sea (SOLAS) 1974. SOLAS was chosen as it is the oldest IMO convention in place and also the most rectified convention by maritime trading nations.

Upon successful compliance to the requirement of the ISPS Code, the port will be issued the Statement of Compliance for Port Facility (SoCPF) for port facility that complied with the requirement. The certificate has the validity period of not more than five years and subject to annual endorsement by the designated administration. For the purpose of ensuring continuous relevancy of the SoCPF, the administration set out the mandatory requirement for subjecting port facilities to undergo periodical external and internal audit. A full compliance is a must
which mean that any non-conformance and/or observation must be closed immediate or the certification will be withdrawn. The consequences of failure to retain the validity of the certificate may result in the vessel being barred from entering into the port area for ship and for the port facility, it would result in the port being shunt by the shippers and freight forwarder. As the cargo loaded from non-compliance port facility would likely to be delayed at the destination port due to unrecognised security measures during loading and will be subjected to further inspection by the port state and in some case the carriers itself also be subjected to further delay and inspection. In worst case scenario, the vessel concerned may be dispelled from the port and the cargo would not be allowed to land.

**Security Risk vs Safety Risk**

The requirement for port facility to carry out risk assessment in compliance to the ISPS Code (IMO, 2003) is stipulated in Part A Section 15 of the Code where in Section 15.1, it stipulate that risk assessment is an essential and integral part of the process in the development and updating of the port security plan (PFSP). The word “updating” is use to reflect the criticality of continuous security risk assessment as the PFSP must remind relevant at all time and its effectiveness being assess periodically. The similar recommendation can be found in other ISO’s documents (28000, 28001, 28004 and 20884) relating to implementation of security measures in logistics and supply management.

It has to be emphasis that there is a distinct differentiation between security risk and safety risk, safety risk or safety related accident or incident is generally the outcome of the failure in the internal organization as well as to those involved in the activities related to that organization. The occurrence of a specific undesired event in any safety incident is the outcome from the internal deviation from the stipulated/agreed standard/s that was based on industry best practices, previous experience, identified risks, availability of technology, training and education as well as other available means identified earlier during risk assessment initiative as well as determined management approach to contain the identified risk. Safety risks can be controlled through internal intervention such as standard working procedures, education, training, drill and exercises. In security risk, the undesired event is the outcome of an intentional act by individual or organized party with the objective of causing loss of life and/or injury, economical losses and/or environmental damages to specific target,
local and even community wide damages. This act will be further realised with the capability of such individual, organization and coupled with their objectives. The objective can be monetary in nature or ideological in purpose. Figure 1 demonstrated the changing security environment the poses security threat to facilities around the world.

Figure 1: Changing Security Environment by Jane’s 2002

For port facility, one area that of great concerned is the location. For mobile facility, such as ships, they are continuously moving around depending on where the demand are whereas port facilities will always in a designated location and when it comes to implementing specific security measures, they always within the preying eyes of the criminals or terrorists, which will allow more time for monitoring the activities concerning security to be monitored and develop the trend be analysed to determine any weaknesses. One good example is the main access point in some port facility where the access for visitors, staff as well as contractors are located in a same locality and when there is peak period, all security personnel are posted at the main entrance to assist in the clearing of traffic. At this point in time, security personnel role are more toward traffic control rather than identifying suspicious person with intention to gain illegal access into the facility and with the focus on the main access, the surrounding perimeters are not being monitor thus allow another opportunities for infiltration.
**Security Risk Assessment According to ISPS Code**

In Part A Section 15.5 of the ISPS Code, provides a clear guide on the 4 elements to be considered when carry out the assessment. They are stipulated as follow:

“The port facility security assessment shall include, at least, the following elements:

.1 identification and evaluation of important assets and infrastructure it is important to protect;

.2 identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;

.3 identification, selection and prioritization of countermeasures and procedural changes and their level of effectiveness to reduce vulnerability; and

.4 identification of weaknesses, including human factors, in the infrastructure, policies and procedures.”

The first element describes the assets and infrastructure that must be included in the assessment and for that purpose, PFSO must first identify the important infrastructure relevant to the nature of operation in the port. The team that carryout the assessment must have a clear knowledge and understanding of the entire operation of the ports such as the nature of cargoes/goods they handle, types of the vessels calling the port, handling, stowage, packaging, warehousing of dangerous and hazardous materials, lines of communication internally and externally, monitoring of movements of vehicle and prime movers within the port, government agencies operating within port area such as custom and immigration, movement of crew, visitors, contractors and own staff, location of critical safety and security facility, monitoring of vessels movement, and many more. For practical purposes, the team need to actually go to the ground the evaluation the actual surrounding and environment at the time of pre-assessment and preferably this carry out at daytime as well as night time. For the berth areas, it is recommended that the team also see the physical condition from the sea approaches. Part B Section 15.4 provides the general guideline on the area of discipline for the expert assistance team members. These activities may varies from port facility to port facility, thus one of the reason why the port facility security plan is only specific for a particular port and no two ports will have similar plan. The gathering of the pre-assessment data is critical as it will provide a clear direction as to what extent the criticality of the assets
and infrastructure to the commercial activities of the port facility and its contribution to overall performance of the port facility. For the security expert, they will be able to relate the possible undesired events may experience by the organization or individual, as these can be the potential target that would result in the most severe extent of damage to properties, human life and environment. Thus it is essential for effective assessment of the facility, the team need to go on the ground, desk top assessment may not provide a good approach in identifying critical infrastructure and assets that might be potential target of attack. It were observed that quite commonly, some facility have a very perimeter fencing placed at the perimeter boarders but unfortunately the drains leading outside of the facility are not being grilled which left it vulnerable for infiltration.

The second element is related to the linkages between the critical infrastructure and operation to the possible threat that the port facility may be exposed to. Part B Section 15.11 of the Code provide possible types of threat that a facility might be encountered but caution must be put in place as any possible threat which likely to be encountered must be addressed by the port facility. Thus any identified threats must be supported by credible information or data. Table 1 below demonstrates the possible threats that port facility may consider to adopt during the risk assessment process and it is noted that the nature of threat that likely to occur is the act that might be demonstrated by the intended party and not any specific individual or organization such as pirate, terrorists or criminal but the acts that could lead to the security risk of the port facility. As mentioned in the earlier paragraph, threat/s are the focal point that beyond the control of the port facility unlike safety risk, the dynamism of the hazard is in the hand of the individual or organization with the intention to activate it and it is an intentional act/s and multiply the effect with the capability of the individual or groups as well as vulnerability of the particular facility.

<table>
<thead>
<tr>
<th>No.</th>
<th>Part B Section 15.11 of the ISPS Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.</td>
<td>damage to, or destruction of, the port facility or of the ship, e.g. by explosive devices, arson, sabotage or vandalism</td>
</tr>
<tr>
<td>.2.</td>
<td>hijacking or seizure of the ship or of persons on board;</td>
</tr>
<tr>
<td>.3.</td>
<td>tampering with cargo, essential ship equipment or systems or ship’s stores;</td>
</tr>
<tr>
<td>.4.</td>
<td>unauthorized access or use including presence of stowaways;</td>
</tr>
<tr>
<td>.5.</td>
<td>smuggling weapons or equipment, including weapons of mass destruction;</td>
</tr>
<tr>
<td>.6.</td>
<td>use of the ship to carry those intending to cause a security incident and their equipment;</td>
</tr>
</tbody>
</table>
.7. use of the ship itself as a weapon or as a means to cause damage or destruction;  
.8. blockage; of port entrances, locks, approaches etc; and  
.9. nuclear, biological and chemical attack.

Table 1: Possible threats recommended in Part B Section 5.11 of the Code.

The third element focuses on the development of countermeasures and procedures as barriers to the possible threats that are likely to be encountered by the port facility. In security risk, it equation as follows:

\[
\text{Security Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequences}
\]

Threat and consequences are beyond the control of the port facility and the only area that is within the control of the port facility is the vulnerability part. Vulnerability generally depends on the effectiveness and completeness of the barriers put in place to safeguard specific potential targets as identified in the first two elements above.

The final element is the overall process of security assessment by combination of data collected and carryout analysis to determine the weaknesses in the presence practices, procedures as well as policies in the organization. This would include the outcome of interview conducted with existing security personals as they are the one on the ground and understand the challenges in executing physical security measures. Some of the common weaknesses relates to human elements are:

- Security personnel training and competency;
- Safety or Personal Protective Equipment not being provided to security personnel on patrol;
- Long hours of work and fatigue, lack of man power;
- Living quarter too far from the area of work;
- No proper means to carrying out patrol and response;
- Lacking of security awareness and response requirement for port staff;
- Security equipment – competence personnel, maintenance, limitation, spares, response procedures etc.; and
- Complacency, situational awareness and others.
Figure 2 is a diagram demonstrating the security assessment process flow where the four elements as mentioned in the Section 15.5 are illustrated. The requirement of the security plan are the identification of possible risks or threats, preventive measures and procedures in relationship to the identified threats as well as procedures and measures in responding in situation where the occurrence of the said risk or the failure of the preventive, thus emergency preparedness activities must also be developed as part of the security plan. In short the PFSP need to covered all the preventive, response and consequences management. Taking that into consideration, the Bow Tie approach (Figure 3) is the most suitable platform to judge the relationship in term of identified threats as well as linking it to the mitigation initiatives in cases of subsequent failure in the prevention measures. This is necessary so that the consequences management is also taken into consideration and taken as part of the assessment.

Figure 2 – Security assessment flow diagram

The figure 3 provides the generic diagram of the utilization of the Bow Tie concept with the Tripod analysis in the study to determine the effectiveness of the security performance for a port facility in term of risk assessment and management of risk for failed security barriers.
Threat Identification

The threat identification methodology utilised for this paper is the one recommended by ILO’s Code of Practice on Security in Ports (ILO, 2003) with additional elements of data coverage to provide a more systematic assessment. The ILO’s security assessment methodology was chosen as it is the recommended methodology by the Marine Department Malaysia and majority of the marine facilities in Malaysia conduct their security assessment based on this methodology.

Figure 4 illustrate the identifications of security risk will commence with the inventory of port activities available in the port facility where it is divided into four difference categories namely operation, facilities, infrastructure and commercial or business entity. In operation, its cover the entire marine related activities such as loading and unloading of goods/passengers including the transfer of goods, movement of vessels in and out of the port or piloting movement, physical movement of goods or stevedoring, handling of dangerous or hazardous goods including chemicals and petroleum products, and handling of goods while in transit such as storage, warehousing, packaging and value adding activities. As these operations may be varies from the port to port based on the area of specialization and focus. The PFSO will need to have full understanding of the port operation to develop the inventory. The next related activities that will be taken into consideration are the physical facilities that facilitate
the activities of the port such as such as berth spaces for vessel berthing and unberthing and the activities in ship-port interface to facilitate the movement of goods and /or passengers, warehouses for storage of goods beside supporting other activities such as packaging and value creation, container yards, access points for vessel including the navigational aids and vessel traffic information and monitoring system, physical perimeter fencing on the shore side including fence lighting and remote monitoring facilities, physical information communication and technology network and other facilities that contributed to the smooth and efficient operational activities.

The other two are the infrastructure and commercial/business information data. These two may not directly contributed to the effective movement of goods/passengers in the port facility but their existance are to ensure the connectivity as well as to provide continuous safeguarding and mitigate any unforseeable consequences of interrupting the effective physical linkages. The infrastructure in focus are roads and access such as bridges and rail track, water access areas so to ensure sufficient underkeel clearance and good anchoring holding ground free from any obstructions, berthing facilities such as mooring bitts, fenders, fresh waterline etc., lifesaving and fire fighting and prevention facilities such as lifebuoys with lights and lines, portable and fixed fire extinguishing system, fire and smoke detection. Finally on the commercial/business information data, refer to the software to facilitate the smooth movement of goods and containers, measuring and monitoring the loading/unloading and transfer of dry and liquid bulk, containers planning , ships’ bending moment and shearing forces diagrams etc.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Facilities</th>
<th>Infrastructure</th>
<th>Commercial/Business Information Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Berthing/Unberthing of vessels</td>
<td>• Berths/Jetty</td>
<td>• Roads and accesses</td>
<td>• Software</td>
</tr>
<tr>
<td>• Piloting</td>
<td>• Warehouses</td>
<td>• Water areas/access</td>
<td>• Computer room</td>
</tr>
<tr>
<td>• Move of goods including dangerous goods</td>
<td>• Container yard</td>
<td>• Berthing facilities</td>
<td>• Data accessibility</td>
</tr>
<tr>
<td>• Identification of personnel and vehicles</td>
<td>• Access point/main and additional</td>
<td>• Safety FFA &amp; LSA</td>
<td></td>
</tr>
<tr>
<td>• Warehousing/storage/packaging/value adding etc.</td>
<td>• Perimeter fencing</td>
<td>• Storage areas</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Entrance gates</td>
<td>• Admin and office site</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ICT and Network</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Figure 4 – Diagram of Port activities

Figure 5 is on Potential/Critical Target relates to port activity. The potential target (PT) are refer to as critical assets, infrastructure or persons in the port and in the immediate environments, that may, if subject to an unlawful act, detrimentally impact on the security, safety of personnel or function of the port (ILO, 2003). As each activity will require support of these critical assets/infrastructure and any attempt to interrupt the routine operation of these assets/infrastructure or personnel would affect the port routine operation. Thus any individual or group with the desire to cause undesired event would target these key points or personnel to achieve their goals or objectives.

![Diagram of Port activities]

Figure 5 – Potential/Critical targets for each port activity

Each asset or personnel identified as potential target will be assessed in term of its criticality. Criticality is refer to the effect to the port in cases which these assets or personnel are being forcefully or unlawfully removed from the routine support element as well as the ability to recover if such incident occurred. The criticality of particular asset or personnel is classed under three categories, namely minor, significant and major. The deliverables are illustrated in Table 2.

<table>
<thead>
<tr>
<th>Criticality Level</th>
<th>Measurement criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor</td>
<td>Has the ability to recover with little intervention and can be brought back to operational status with shortest possible duration (Less than 24 hours) by mean of immediate replacement of identical unit, availability of secondary unit with similar capability or ability to</td>
</tr>
</tbody>
</table>
Table 2: Measurement criteria for criticality levels.

Figure 6 is a simplify flow diagram on how the possible threat is identified and its severity is assess. This box describe the possible scenario that can occure to the potential target if unlawful or undesire attempt is made on the potential target. This requirement is stated in Part B Section 15.9 to 15.11 of the Code.

Figure 6: Qualitative approach of identification of criticality level base on possible threat scenario

An example (reference to Figure 6) of possible threat to a facility is successful gaining unauthorized access to a port facility. In this case the PFSO will first determine whether such
an occurrances occurred before in the port facility based on existing record. If it was noted that such occurrences occurred before, most likely that the facility would have the measures in-place to prevent future occurrences. The second level after the first arrow demonstrate the likely objective of such an intrusion, and if it is a successful attempt, what would be the outcome. This flow diagram provide the overall flow of a particular threat linking the criminal act with the objectives of the intention and its consequences of a successful attempt to determine the level of possible threat that might be posed on specific PT.

<table>
<thead>
<tr>
<th>Scenario No.</th>
<th>Threat Scenario</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Impact</th>
<th>Risk Score</th>
<th>Action priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
</tr>
<tr>
<td>1</td>
<td>Destroy port authority's communication tower by explosives</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Example of TRAM table.

Once the threat level, vulnerability and the consequences/impact are determined, the levels are specified using the range scale recommended by ILO’s TRAM. The ILO recommendation for determining of level of impact provide a better apportioning of scoring as the division of criteria provide flexibility to distance the victims from the potential target as part measures to reduce the risk score as one of the element that mentioned in part A Section 16.3.5 of the ISPS Code.

Under the ILO recommendation, the common challenge faced during the security assessment is the determining of level of acceptable risk score. Based on ILO recommendation, acceptable risk score is not mentioned to guide further mitigation initiatives. As the risk score is derived from multiplication of result in threat, vulnerability and impact assessment, any single changes in the score would generally double the risk score and as the ranges of threat, vulnerability and impact are various for all three deliverables, the equal ranges separation of division cannot be applied to equate it to the recommendation by USCG on assessment outcome as Document, Considered or Mitigate. In this case, the port facility will has to determine the result of acceptable risk score in term of percentage, example allowing 5% of the highest score (which is 60) as acceptable risk score where no further action is required or allowing 5% gap and any outcome more than 5% mean additional initiative of enhancing
existing security measures or barrier/s need to be put in place or even place additional new security barriers or measures.

**Effectiveness of Security Measures and Procedures**

For the purposes of evaluating the effectiveness of the security measures and procedures implemented by the port, drills and exercises is one of the mean recommended in Section 18.3 of the Code. But in Part B Section 18.5, minimum recommended period of drill is at least once every 3 months and for exercise (Part B, Section 18.6), one every calendar year with the distance between exercises not more than 18 months. Based on Part A Section 16.3 of the Code, there were altogether 15 areas that the PFSP must covered and in MSC circular 1131, there were altogether 93 sub-parts that must be dealt with by a port facility. It will take 23.25 years for a port facility to put these security measures and procedures into test to determine the effectiveness.

Tripod-Beta may be the methodology which can be applied to identify possible failure in each security barrier and identify whether these possible failure in the security barriers were recognised by the management of the facility and preventive actions were in-place to ensure sufficient supports were provided to ensure these security barriers do not collapsed. For each security barriers in-placed to provide protection to the potential target, the possible immediate cause to the barrier failure is identified and this is known as active failure. Pre-condition is where the contributory factor/s that may cause the failure and the Latent failure is the root cause/s that contributed the this overall failure and in most cases that may be leading to the failure of management to provide effective support. This approach is recommended based on account that the major elements that is within the control of the port facility against any possible threat is its vulnerability and the raise or down grade of the vulnerability lies sole with the port facility as the first line of defence whereas intervention by government security agencies generally will be based on intelligent information received at the time and after event response, which would likely be too late in term of avoiding damages. In most instances, single security measure will be able to provide solid security barriers against any possible threats and at the same time, any security barriers would require organization commitments to materialize it. These commitments will be based on the nature of barriers put in place. For example, if security personnel are position at the guardhouse to monitor the movement of vehicle accessing the facility and at the same time to ensure no unauthorized
person gaining access into the facility. The port facility need to ensure that the security personnel are trained in identifying and recognising behaviour of suspicious person or vehicles, parking bays are allocated outside the guardhouse to allow sufficient time for security personnel to verify the driver identification and contact relevant person in the facility without obstructing the incoming vehicles, physical barrier such as vehicle post is position at the gate to inform approach vehicle that they have to stop and obtain permission before access, clear signage before the entrance to let the vehicle know that they are approaching a restricted are.

<table>
<thead>
<tr>
<th>Security Measure</th>
<th>Active failure</th>
<th>Pre-Condition</th>
<th>Latent Failure</th>
</tr>
</thead>
</table>
| Procedures to prevent unauthorized person and vehicle accessing the port facility | • Training of security personnel  
• Vehicle waiting area  
• Guard post/barrier  
• Signage | • Training need analysis  
• Threat and risk identification | • Company security policy  
• Management support |

Figure 7 – Structure for identification of performance gaps

Figure 7 is an example of the initiative needed to prevent access of unauthorized person and vehicles to a port facility.

**Summary**

It is critical that port facility security assessment be done in systematic approach as the scope of port activities are vast and varies, and in present competitive commercial environment, security is one of the component of performance that determine the attractiveness of the port facility as any delay would be the push factor for the potential client to go for another more secure port. The PFSP is a preventive plan and risk assessment is the mean to ensure that the coverage of the plan is in totality and all possible threats that likely to occur in the port facility are taken care off. A strong assessment team would provide the totality in all aspect be it operational, human resource and management support, to ensure the completeness of the plan.

Compliance alone would not be sufficient to the present setting as the enemy will always study their opponents and any vulnerability in the system will likely be noticed in manner of time and a new approach will be devised. Thus is it vital that the port facility continually assess its effectiveness of the security measures and procedures in place.
References:


