CHAPTER 6

Security

This chapter provides a brief summary of the requirements of the *International Ship and Port Facility Security (ISPS) Code* and industry best management practices and guidelines.

6.1 General

Internationally trading ships, and terminals handling such ships, are required to take measures to enhance maritime security and to comply with the provisions of the ISPS Code Parts A and B. The ISPS Code applies to shore based facilities in States that are party to the SOLAS Convention. Industry best management practice and guidelines for improving security should also be considered.

It is recommended that all tankers and terminals conduct a thorough security risk assessment and develop a security plan. Tankers should also develop a hardening plan. The security plan should include procedures, measures and controls to address all identified security risks.

Tankers and terminals that are not required to comply with the ISPS Code are still recommended to consider its requirements, along with industry best management practices, when developing their security plans.

6.2 Threat and risk assessment

To fully understand the security risk, conduct a risk assessment of all security threats. A threat is formed of capability, intent and opportunity, as shown in figure 6.1. The risk is a function of the threat, coupled with the vulnerability of the asset and the consequences of the incident.

Figure 6.1: The threat triangle

Removing one side of the triangle will minimise the risk.

Capability means attackers have the physical means to attack. Intent is demonstrated by the will and means to attack. Opportunity can be reduced by the company, tanker and terminal operators through security plans. Ask regional or local authorities for more information about threats, e.g. region specific threats, new tactics and mitigation measures.

6.3 Security risk assessments

The security risk assessment should include all tanker and terminal operations and should identify:

- Areas most vulnerable to attack.
- Key areas to be protected.
- Threats and likelihood of occurrence.
- Consequences of an attack, including to other tankers at berths or at anchor.
- Measures for preventing, mitigating and recovering from an attack, including provisions from the ISPS Code and other additional measures.
- Any weaknesses in existing security measures, procedures and operations, including human factors.
- Personnel responsible for carrying out security measures.
- Methods or means of communicating that an attack is underway.

6.4 Cyber safety and security

Cyber security is concerned with the protection of Information Technology (IT), Operational Technology (OT), information and data from unauthorised access, manipulation and disruption. Cyber safety covers the risks from the loss of availability or integrity of safety critical data and OT.

The cyber security risk assessment should consider threats to cyber safety and cyber security, because attacks on either can harm personnel, the environment and the tanker or terminal.

The IMO has adopted resolutions on Maritime Cyber Risk Management (see MSC-FAL.1/Circ.3 *Guidelines on Maritime Cyber Risk Management*). Effective cyber risk management starts with senior management, who should develop a culture of cyber risk awareness at all levels of an organisation. For practical guidance for Masters and ship's crew, see industry *Guidelines on Cyber Security Onboard Ships*, and ICS/BIMCO/Witherbys' *Cyber Security Workbook for On Board Ship Use*.

6.5 Security plans

A security plan should be written for each tanker and terminal and should describe:

- Who is responsible for carrying out security measures.
- Security organisation.
- Security training and drills.
- Basic security measures for normal operation.
- Additional measures that will allow the tanker and terminal to respond quickly to changes in threats, e.g. by reducing or increasing the level of security.
- Procedures for linking tanker and terminal security activities with the security activities of port authorities, other tankers, terminals and facilities in the region and other local authorities and agencies, e.g. police and coast guard.
- Arrangements for regular reviews of the security plan and for amendments based on experience or changing circumstances.
- Access control measures.
- Measures to prevent unauthorised weapons, dangerous substances or devices intended to harm people, tankers or terminals being taken onto the tanker or into the terminal.
- Procedures for responding to security threats or breaches of security, which may include evacuation.

6.6 Responsibilities under the International Ship and Port Facility Security Code

The port is responsible for security and must appoint a Port Facility Security Officer (PFSO) who may be designated one or more port facilities (terminals) and is responsible for the port security plan. The person should be trained and capable of implementing all security measures.

For tankers at a terminal, while the PFSO is responsible for the port security plan, the Master has overriding authority to make decisions about the safety and security of the tanker. A Ship Security Officer (SSO) should be appointed who is trained and capable of implementing the ship security plan and security measures on board. The SSO could be the Master but is often one of the senior officers.