CHAPTER 8: PORT SECURITY PLANNING

PORT SECURITY APPLICATIONS OF SYSTEMIC RISK ANALYSIS

A comprehensive security risk analysis for port and marine intermodal freight movement can enhance the ability of port security managers to execute their risk management responsibilities. It is an important tool for documenting, monitoring, and assessing the impact and effectiveness of the security systems and crime countermeasures implemented throughout every phase in the shipping cycle.

Effective port security planning can result in the development and implementation of measures to reduce port vulnerabilities. Recognition of potential vulnerabilities must precede development of appropriate countermeasures. Port security management must be capable of ascertaining the nature and magnitude of all foreseeable security threats to the port's operations. Consequently, a comprehensive security survey and risk assessment is the first task in the process of establishing an effective port security regime.

Risk Assessment

The security of a maritime cargo shipping cycle – from the product producer at the source to the consignee at the destination – can be assessed by examining its vulnerabilities in comparison to the threats it faces (e.g., cargo theft, drug smuggling). The quality of the security standards and practices can be measured in relation to intended outcomes by analyzing, documenting, and rating the operational methods of individual shipping and transport facilities, installations, and activities.

Risk Management

Alternative courses of action for controlling risks can be selected by processing the information derived from the risk assessment. The operational flows of the system can be modeled using plausible scenarios to identifying vulnerable transaction points in the shipping cycle and determining root causes of risk (e.g., lax security in freight forwarding operations). This process continues to formulate preventive actions and execution of an implementation plan. By taking a systemic approach, anti-crime security can be implemented, made accountable, and auditable for an entire freight transport system or even international trade corridor to ensure secure and profitable freight movement.

This chapter represents a brief outline relating to a subject on which much has been written. It is provided only as another area the risk manager should address.

The risk management process should include the planning and development of port security. It is an integral facet of the port risk management process. The port security mission is to prevent or minimize injuries to personnel, damage to port property, loss of cargo due to criminal activity, terrorists, or disgruntled employees.

SECURITY ISSUES

All too often ports are concerned only about risks or threats that exist at their port without taking into consideration the activity occurring in nearby or distant ports, which could have an adverse impact on the port. A seaport, by the nature of its business, is a microcosm of the world. Ships travel daily loading, transporting, unloading their cargo from port to port, thereby contributing to the globalization of free trade. As such, world problems can become problems for the port.

Ports generally have certain countries and shipping lines that engage in interstate and international trade. As such, if the shipping line is experiencing losses from employees or criminal activity, these problems can soon become a problem for the port. Likewise, personnel in the ships crew could be part of an organized crime group who engage in criminal activity, transporting stolen goods, drugs, money from one

port to another, as well as from one country to another.

In addition to these losses, ports and shipping lines face assessment of severe financial penalties from government agencies for failure to take strong measures to prevent such occurrences.

It is important for risk managers to be current on security issues in the countries their port is serving and to be knowledgeable of any criminal activity surrounding shipping companies serviced by their port. These issues could easily transfer to the port if proper security measures are not in place.

RISKS/THREATS

Port risk managers face a myriad of risks and threats. They manifest themselves in forms of cargo theft, smuggling of narcotics and currency, terrorism, piracy, stowaways, labor unrest, as well as hijackings. Increasingly cargo theft and the smuggling of narcotics and currency are a growing problem generating significant revenue. Organized criminal gangs, some of whom are multinational and operate in several ports located in a number of countries, may commit these acts.

They target high priced items, such as computers, fashion design clothing, perfumes, and liquor, which are easily sold in the underground distribution network and difficult for law enforcement to trace.

It is not uncommon for the gang to have a "plant" inside the port or shipping company with access to shipping information. These gangs have demonstrated the ability to shift to other ports in continuance of their criminal enterprise when security measures are enhanced at the port in which they currently operate.

Terrorists have used the sea lanes to illegally transport weapons and explosives to terrorist groups in other countries. There have also been incidents where hoax bombs and bomb threats have been directed at a port and ship. These actions were perpetrated in connection with an extortion scheme and for general disruption of port operations. In both instances, port operations were disrupted for a significant period of time.

PORT SECURITY PRE-PLANNING

In development of a port security plan, the port size, content of product and services within the port perimeter must be taken into consideration. When designing your plan, it should reflect feedback not only from the Port Director's office, Directors' of Operations and Security, but also consultation with the U.S. Coast Guard (Captain of the Port); U.S. Customs; Directors' of Planning, Facilities, and Vendor Operations; General Counsel; and emergency service providers (local law enforcement, fire service, and medical).

Discussion should also be conducted with shipping companies and vendors operating on and off the port, who are either serviced by the port or service the port. Their perspective of issues to be addressed should be solicited.

These individuals and groups will have valuable information that will provide for a comprehensive and integrated security plan, encompassing port and vendor operations as well as regulatory compliance.

DEVELOPMENT OF A PORT SECURITY PLAN

Prior to developing a port security plan, a comprehensive physical security survey should be conducted, identifying the port vulnerabilities, assessing risks and threats, and offering methods to mitigate these issues. Such a survey will result in a more cost effective and efficient security plan. The plan should address current as well as future security issues that could arise.

All too often ports address current problems, failing to identify future threats, resulting in reduced efficiency, increased cost, and most probably providing a solution that does not interface with the previous plan.

It is recommended that risk managers develop their plans utilizing a five-step process: *assessment, field interviews, physical survey, internal review,* and issuance of a *formal report.*

Assessment

The *assessment* process includes a detailed briefing from:

- The Port Director's office
- Directors' of Port Operations, Security, Planning, Facilities, and Vendor Operations
- U.S. Coast Guard
- U.S. Customs
- General Counsel
- Emergency service providers such as local law enforcement, fire, and medical services

This briefing level is important to determine what they perceive as problems and vulnerabilities, identification of future port operational plans and expansion, and identification of personnel for field interviews.

Field Interviews

The second step, *field interviews* involves:

- In-depth interviews of key personnel
- Detail descriptions of their responsibilities
- Perception of issues and vulnerabilities.

It has been found that perceptions of issues and vulnerabilities change the further down the management level we proceed.

Physical Survey

In the *physical survey* step, an actual on-site evaluation is conducted to assess:

- perimeter security
- access/egress control
- review of facility security systems
- management information systems which house shipping data
- security personnel

It is important to evaluate perimeter lighting, closed circuit television (CCTV) coverage, alarm systems, and access control to the management information systems (MIS) system containing shipping information. In addition, the communication systems must be assessed to determine if timely information can be transmitted to security forces, to alert them of occurrences within the port, outside the port, and with other pertinent ports.

Furthermore, a risk assessment of the surrounding physical environment and criminal activity should be conducted.

Internal Review

The *internal review* should consist of:

- Reviewing and evaluating current physical security manual/plans and operations
- Assessment of crisis management and emergency management plans to mitigate a security or fire emergency
- A review of business operations

The last process should be preparation of a formal report, either verbal or written, or both. This will be important in documenting your port vulnerabilities, assessing risk, and outlining methods to mitigate risk. The report will be your justification for funds to address the identified problems.

SUMMATION

As you develop a port security plan, ensure that it is comprehensive, methodical, and identifies not only current problems but also projects into the future. When developing the plan, remember it is better to be pro-active than reactive.