Egyptian security

Following on from his review of security issues relating to the Panama Canal, Ronald Thomason now turns his attention to Egypt and the Suez Canal

Ronald Thomason is Vice President - Strategic Programs with the Maritime Security Council and President of Infrastructure Security Solutions LLC. He looked at the security implications of the Panama Canal expansion programme in the February/March issue of *Cargo Security International*.

Contact:
Ronald Thomason
Tel: +1 954 495 7611
Email: rjthomason
@maritimesecurity.org

The turbulence resulting from Egypt's evolving internal political and social dynamics represents a potential challenge to the country's commercial resilience and economic development. As the caretaker for the Suez Canal, one of the world's critical gateways for global maritime commerce, Egypt is extremely sensitive to any real or perceived hazards or threats that may negatively impact the canal's normal operations. In risk management for commercial business operations, confidence in the security, effectiveness, efficiency, and resilience of the mechanisms of commerce is the fulcrum on which global commerce is delicately balanced. Any changes that alter that balance could result in a negative cascade effect on Egypt's ability to engage effectively in global commerce. The severity of the disruption may result in the adjustment of the country's sovereign risk rating. These challenges, however, may be effectively addressed through the application of accepted security standards and practices designed to maintain the security, efficiency, and competitiveness of Egypt's commercial trade and transportation communities.

Changes and considerations

The 1985 hijacking of the passenger cruise ship *Achille Lauro* resulted in the **International Maritime Organization** (**IMO**) developing security standards and practices for passenger cruise ships, facilities, and their operations. Subsequent terrorist attacks against the *USS Cole* and the *Limburg*, off the coast of Yemen, showed how Al Qaeda and the spectre of terrorism posed a very real and significant threat to the commercial shipping industry – not just in terms of their potential for direct attack against specific targets, but also for the disastrous effect such attacks would have on the global economy.

Since then, varied arrays of threats have manifested themselves against the operational elements of maritime commerce and the global supply chain. In addition to terrorism, the spectrum of credible threats may include, but is not limited to, a combination of the following impediments to normal business operations:

- localised natural disasters that can restrict the flow of products via road or rail
- labour unrest at the ports, cargo transshipment, or intermodal exchange nodes
- organised or 'opportunistic' crimes that result in increased losses of product due to 'shrinkage' and increased risk insurance premiums
- political instability that calls into question the country or region's ability or commitment to conduct effective oversight and enforcement of (safety and security) regulations for commerce within its geographic jurisdiction.

Effective business leaders maintain awareness of the risks attendant to their facilities and enterprise operations, and have calculated the point of diminished returns.

When the cost of compensating for or overcoming the identified risks to the company's operations in Egypt approaches the threshold at which the value of the revenue stream is threatened, deciding whether to maintain operations there is reduced to a simple business decision.

The formula for evaluating this important business dynamic is: Threat x Vulnerability x Consequences = Risk. Threats are categorised as all 'hazards' that may degrade or restrict normal business operations. Vulnerabilities include impediments or deficiencies in security infrastructure, policies, personnel, and procedures. Consequences include the quantitative or qualitative determination of the results of an incident or event based on:

- injury or loss of life
- length of delay or denial, and time required for recovery of service
- environmental impact of the incident or event, and the length of time and cost for its remediation
- the cascade effect of the incident or event on supporting or connecting operations.

For example, labour unrest at one Egyptian port may require cargo vessels to be redirected to other ports for

loading or unloading, disrupting vessel itineraries and schedules and creating a kink in the supply chain that may result in just in time (JIT) shipments not being executed as scheduled. All of this costs time and revenues.

Resilience and continuity

Company executives generally focus on the design and planning of facilities and operations required to optimise the opportunities for operational efficiencies and maximum revenues via their overseas operations. An important element of the decision making process, however, should include the conduct of scenario-driven exercises to identify the requirements for effective contingency plans.

The development of effective contingency and continuity of operations plans can only be developed based on valid information on the capacity, functionality, and demonstrated effectiveness of the host community incident response and recovery resources available at each company location. This exercise is best conducted in cooperation with appropriate representatives of the host country's federal and municipal government agencies.

For example, it is important that knowledgeable representatives of the Egyptian government and industry communities participate in evaluating the functional capabilities, mechanisms, and timelines for deployment of emergency response personnel upon changes in the hazard environment or in response to security incidents. In order to accomplish this, the company must first identify the security standards and practices against which its facilities and operations must comply. The security standards, performance objectives, and system and personnel requirements necessary to support operations at all security levels should be documented in a site and facility-specific security, incident response, and continuity of business operations plans. In order to ensure that these plans are maintained, they should be audited against the facility's infrastructure and operations on an annual basis – or any time a significant change has occurred. It is likely that the recent events in Egypt may have resulted in physical or operational changes at Egypt's port facilities, which should have prompted the initiation of security plan audits of their infrastructures and operations.

Best management practices

Following the terrorist attacks in New York, London, Madrid, and Mumbai, a number of international and national security standards and industry best management practices (BMPs) have been developed to enhance the security of global maritime commerce and the global supply chain. Some of the regulatory security instruments that may apply to commercial maritime port facilities, vessels, and offshore platforms include:

- *International Ship and Port Facility Security (ISPS) Code*
- *ISO 28000 - Security for the Supply Chain*
- *Customs-Trade Partnership Against Terrorism (C-TPAT)*
- *UNSCR 1540 – Weapons of Mass Destruction (WMD) Non-Proliferation.*

Each regulatory instrument identifies risk-based security standards, practices and performance objectives designed to facilitate the effective prevention, response to, and recovery from security-related incidents or events. Each industry conducting business with, or having facilities and operations in, Egypt is responsible for addressing the threats and risks specific to their industry, locations, and operations. Of course, adoption of security policies and procedures by companies doing business in or with Egypt will not by itself deter or mitigate the risk of security incidents, or lessen Egypt's obligation to execute due diligence in the oversight and enforcement of the applicable trade and transportation security policies and procedures.

This is best demonstrated through the integration of the applicable security standards and practices into the enterprise security programmes for each company, and tailoring their security plans to include the credible threats, vulnerabilities, and appropriate

'In addition to their concern for the security of the ocean-going carriers of their crude and refined petroleum products, energy companies must also be concerned about the security of their offshore energy platforms, inshore refining and storage facilities'

risk reduction measures specific to their facilities and operations. In addition to their concern for the security of the ocean-going carriers of their crude and refined petroleum products, energy companies must also be concerned about the security of their offshore energy platforms, inshore refining and storage facilities. The security concerns of Egypt's tourism and hospitality industries cannot be limited to passenger cruise vessels and the terminal facilities that support them, but must extend to the land-side shore excursion sites and companies that provide guest transportation between the terminals and the tourist venues.

The consequences of non-compliance with security standards and practices for companies doing business in or with Egypt may include:

- increased exposure to risk of incidents from credible threats
- loss of regulatory and risk rating agency confidence in the effectiveness of enterprise security operations, resulting in increased inspections and reduced cargo throughput
- exposure to regulatory agency sanctions, and lengthy and costly litigation
- loss of brand reputation and integrity.

The Egyptian government retains responsibility for implementing a security programme that identifies the standards and practices for commercial business operations that fall within its purview. It is also responsible for conducting oversight of security training, drills, and exercises programmes in a regular and recurring fashion, to ensure their compliance with the identified security standards and practices at all enterprise levels. Therefore, implementation of a programme that demonstrates 'functional compliance' with all the applicable security standards and practices will significantly reinforce investors' and trading partners' confidence in the security, operational effectiveness, and resilience of Egypt's trade and transportation communities.

Fundamental element

Security should be considered as a best business practice, and be included as a fundamental element of any company's equation for establishing the viability of developing and conducting commercial operations in Egypt.

'Implementation of a programme that demonstrates functional compliance with all the applicable security standards and practices will significantly reinforce investors' and trading partners' confidence in the security, operational effectiveness, and resilience of Egypt's trade and transportation communities'

Since any chain, including the global supply chain, is only as strong as its weakest link, it is important that the company operations, security, and risk management executives know what questions to ask in order to support their ability to make informed business decisions on their foreign operations. While a good due diligence inquiry will be tailored to challenges and limitations of the operations in a specific region or site location, general questions should include:

- which international and national security regulations apply to your company's Egyptian facilities and operations?
- do you and your enterprise partners have published security policies and procedures that identify the prevention and mitigation requirements for the credible threats to your facilities, personnel and operations in Egypt?
- are security threat, vulnerability, and risk assessments conducted of your company and its Egyptian enterprise partners' facilities and operations?
- does your company conduct regular and recurring security awareness and regulatory compliance training, and drills and exercises for its personnel at all enterprise levels?
- are your risk managers aware of the level of exposure to you and your enterprise partners, specifically the risks of legal and financial liability resulting from a transportation security incident?

Finally, it is important that companies considering doing business in or with Egypt develop a comprehensive risk mitigation programme that includes the following key elements:

- a consolidated spreadsheet of security regulations applicable to their enterprise facilities and operations
- comprehensive threat, vulnerability, and risks assessments conducted for each facility's location and operations, conducted on a recurring basis
- a security plan that addresses the compliance requirements based on the applicable security regulations as identified in Egypt's security programme, and documented in the company's own security manual
- a plan that provides security awareness and compliance training, drills and exercises for company personnel at all levels of management and operations
- a programme for communication with government and industry organisations to maintain a current and accurate awareness of credible threats necessary to support an effective company security risk mitigation programme.

In order to sustain Egypt's growth and economic development, it is essential that there is a commitment, from both the highest level of the Egyptian government and industry leaders, for investment in programmes, systems and personnel necessary to ensure the security, operational efficiency, and resilience of their commercial enterprise partner facilities, personnel, and operations.