ENERGY SECURITY

Security for the Energy Industry

by Ronald Thomason, President of Infrastructure Security Solutions LLC

The recurring sound gradually intruded into his dream, drawing him reluctantly into a state of semi-wakeful consciousness. The mobile phone's ringtone indicated the call was from his company's operation center manager, and it seemed to include a note of urgency that was reinforced by the time reflected on his nightstand clock. Two-thirty, he thought, why can't crises happen during normal business hours, or at least until after my first cup of coffee? With a growing sense of foreboding, he picked up the phone. "Yes?"

"Sir, this is the Incident Management Center Director calling to notify you of an incident and advise you that, in accordance with company policy, you or your alternate are required to report here as soon as possible."

"Good morning. Is this another one of the incident response drills that's designed to meet our insurance company's safety compliance requirements?"

"No sir, this is not a drill. We're receiving reports of an actual incident related to the Niger Delta operations."

He was wide awake now. He'd run through the next sequence of questions in his mind since the incident response drills his company's CEO and Board of Directors insisted on following the offshore energy platform the previous year.

"What kind of incident… was it shore side or on a platform? What is the preliminary damage estimate? Was anyone injured? Was production interrupted and, if so, is there any indication of how long it will be until full production capacity is restored?"

"Wait…sir we're receiving another…no two more reports on additional incidents in the same area!"

"What are you saying? What is the exact nature of these incidents that requires headquarters to respond at this ungodly hour? Can't this be handled by the local or regional operations and incident response people?"

"Well sir, as of this moment we've received reports of a breach of one of the oil transmission pipelines that connects the offshore platform to the storage tanks; the apparent explosive malfunction of two power transformers that support the pumping control station; and the workboat scheduled to deliver platform crew replacements and supplies is more than two hours behind schedule."

"Each of those things could be an accident or maintenance issues. As for the service boat, that may easily be a case of the vessel pilot operating on Africa time. You know, the American concept of adhering to time schedules is not one the vessel operator's strong points."

"Well sir, while any one of these events alone is not sufficient to cause concern, three happening in such close chronological and geographic proximity to each other suggests they may be part of a coordinated series of attacks. As such, I felt it was necessary to activate our incident response protocols until the threat can either be confirmed or discounted."

"Have we received any threats, demands, or any other indications that this is anything other than a series of accidents and a case of poor maintenance on the platform service vessel?"

"No sir… but I don't believe in coincidence, especially since the events all seem to be focused on our energy production facilities and transmission operations. In my opinion, we need to take immediate action to prevent further damage to our facilities, reduce the exposure of our people to possible injury, and protect the company against risk of legal and financial liability."

"Okay, please continue following the protocols in our incident response plan and I'll be there within the hour."

THE OPERATIONAL ENVIRONMENT

This is the environment in which the energy production and transportation industries operate on a daily basis. The economies of the world's industrial nations, and those pushing hard to join that club, are dependent upon energy resources to fuel their growth and economic development. In today's global economy, the trade and transportation systems that support international commerce are fueled by petroleum products, and any interruption or threat of interruption in the availability of that essential commodity can have an immediate and debilitating cascade effect on the economies of countries all along the supply chain. Given the global nature of the energy industry, the weakest link in its operations resides in its systems for the transportation of energy products from the point of production through each of the nodes for refining, storage, distribution, and ultimately point of sale.

CREDIBLE THREATS

The security threats arrayed against the energy industry are dynamic and represent a broad range of general and specific interests that may manifest themselves against the weakest link in the energy industry's global supply chain. Separatist groups with nationalist political objectives may engage in actions against energy facilities and operations run by multinational enterprises to express their discontent with

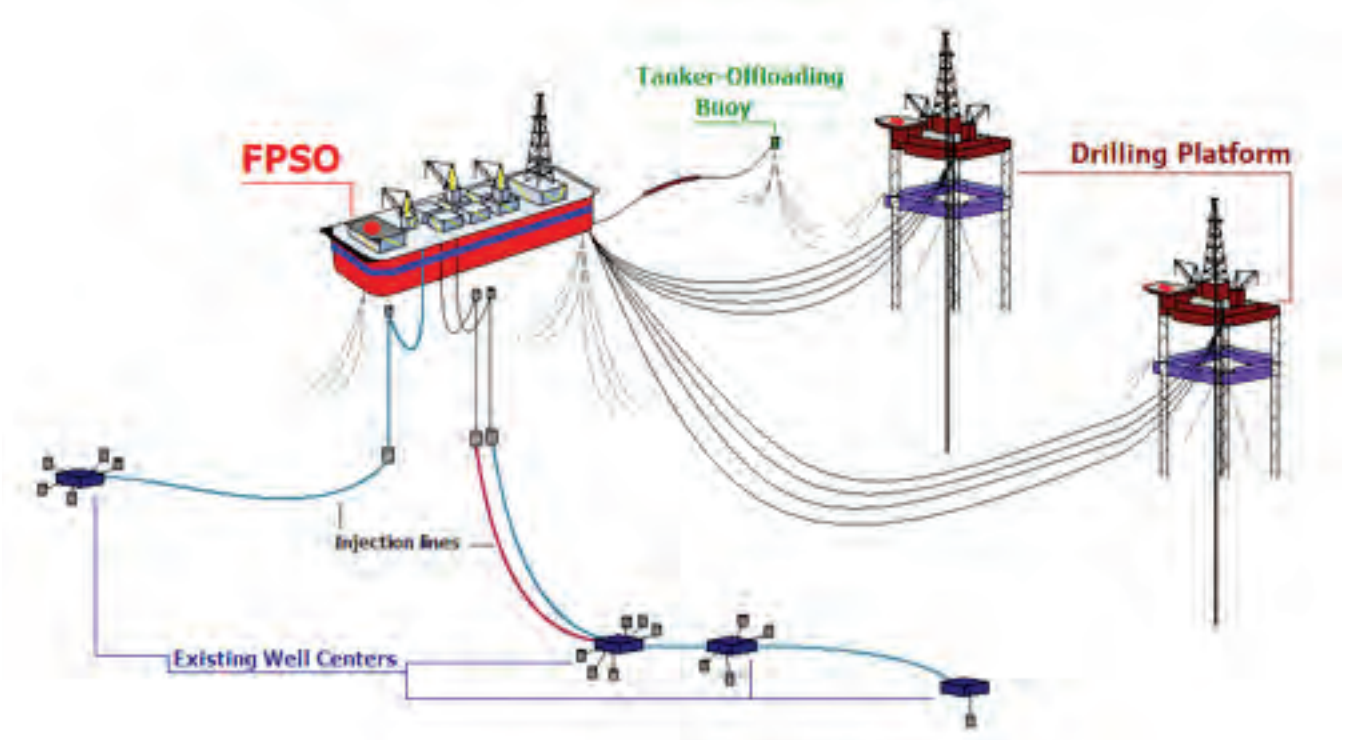
the perceived inequitable distribution of revenues resulting from the exploitation of their national resources. Environmental groups may target pipeline transmission facilities or maritime carriers in protest against their perceived negative impact against the environment in which they operate. Energy company service vessels and employees may be kidnapped and held for ransom purely as a revenue-generating enterprise by individuals or organizations with criminal intent. And finally, groups like al-Qa'ida have targeted the energy supply chain for attack as a method of weakening the economic ability and determination of nations they consider adversaries of Islam to sustain the "war against terrorism."

The unfortunate reality is that threats against the energy industry do not have to manifest themselves in a dramatic fashion, such as a vehicle borne improvised explosive device (VBIED) attack against a petroleum transportation ship, offshore platform, or tank farm to have the desired effect. The volatility of the energy community is such that any incident that interrupts the flow of oil through the supply chain or even the threat of an attack is sufficient to result in an increase in the price of crude oil on the international spot market, as well as at the neighborhood service station. How then, given the far-flung scope of these enterprises and the extremely dynamic nature of the threats, can the energy industry protect the integrity of its facilities and operations, ensure the well being of its employees, and implement effective protective measures in the most cost and operationally-effective manner possible?

Important steps in implementing effective security programs for energy industry systems and operations include identification and prioritization of "single points of failure" in their industry critical infrastructure key assets and operations that may be vulnerable to attack. Next is identification and quantification of the threats at each of the energy company's locations, and the risks and consequences associated with those threats.

"Our enemies are fully aware that they can use oil as a weapon against America. And if we don't take this threat as seriously as the bombs they build or the guns they buy, we will be fighting the War on Terror with one hand tied behind our back."

— President Barack Obama



Once these critical steps are performed the next challenge facing multinational energy companies is integrating the information developed in the analysis of the threats, vulnerabilities, and risks into consolidated, enterprise-wide risk mitigation programs that will enable the company to deter, detect, respond, and recover effectively from incidents or attacks. But how is this done, and where does one start?

REGULATORY ENVIRONMENT

Subsequent to the events of 9/11, the UN's International Maritime Organization (IMO) developed the International Ship and Port Facility Security (ISPS) Code to provide security standards and performance objectives for the international maritime community, which applies to commercial maritime port facilities, vessels, and offshore platforms. Subsequent targeting of maritime energy carriers, transmission pipelines, and energy platform service vessels by criminal and terrorist organizations led to the development of additional regulatory instruments whose application may be focused on the energy products, or the mechanisms by which they are transported through the supply chain. In addition to the ISPS Code, some of the security regulations and industry "best practices" that have emerged and may be applied to the energy industry include:

- *US Maritime Transportation Security Act (MTSA);*
- *Counterterrorism Chemical Facility Anti-Terrorism Standards (CFATS);*
- *Customs-Trade Partnership Against Terrorism (C-TPAT);*
- *UNSCR 1540 – WMD Non-Proliferation;*
- *Pipeline Hazardous Materials Security Act (PHMSA); and*
- *ISO 28000 - Security for the Supply Chain.*

All of these instruments outline security standards and performance objectives that provide a framework for the development and enterprise-wide implementation of effective security policies and procedures. Of course, the adoption of security policies and procedures by energy companies will not by itself deter or mitigate the risk of security incidents, or lessen the company's obligation to execute due diligence in the execution of those policies and procedures. Due diligence is defined and demonstrated by adapting the company's enterprise-wide security policy and procedures into security plans that reflect the threats, vulnerabilities, and recommended risk remediation measures specific to their individual enterprise facilities and operations.

The ability of those company facilities to execute the procedures in their security plan is reflected in their program for conducting security training, drills, and exercises for their personnel at a local level. Non-compliance by an individual energy industry facility may compromise the integrity of the entire supply chain, and expose the company to an increased risk of legal or financial liability in the event of a security incident resulting from deficiencies in their energy transportation system's protective measures. Since the capabilities and intent of the threats against the energy industry are dynamic and constantly evolving, there is no one solution that can effectively address them across any one company's operational spectrum. Therefore, it is critical that the company have security professionals at each enterprise level and at each facility that has a thorough understanding of the applicable security regulations, and is practiced in the implementation and oversight of the company's security policies and programs. A comprehensive risk mitigation program will include the key elements:

- *A consolidated spreadsheet of security regulations applicable to the energy companies facilities and operations;*
- *Security threat, vulnerability, and risks assessments conducted for each enterprise facility and its operations conducted on a recurring basis, the frequency of which is dependent upon the facility's evolving threat profile;*
- *A security plan that addresses the compliance requirements associated with the applicable security regulations, as outlined in the policies and procedures captured in company's enterprise security manual;*
- *A training plan that provides security awareness and compliance training, drills, and exercises for company personnel at all enterprise levels;*
- *A program for communication with industry and government organizations to obtain threat information necessary to support an effective company's security risk mitigation program; and*
- *The commitment, at the highest level of corporate leadership, for investment in security programs, systems and personnel necessary to effectively address the ongoing threats facing the energy industry worldwide.*

The energy industry has an obligation to its employees and shareholders to apply appropriate and effective preventive security, incident recovery, and continuity of operations programs that are tailored to the credible threats at each enterprise location. Individual enterprise investment in comprehensive risk mitigation programs is the best way to address weaknesses in their respective segments of the energy supply chain, where their vulnerabilities can expose the entire industry to the risk of interruption, and reduce the trigger mechanism for escalating prices at the pump.

The Author

Ronald Thomason is President of Infrastructure Security Solutions LLC, a provider of security consulting services for the maritime trade and transportation communities worldwide. Mr. Thomason also serves as the VP of Strategic Programs for the Maritime Security Council.