RiskWatch

www.riskwatch.com

Oil and Gas Industry

A Comprehensive Security Risk Management Approach

Introduction

This white paper explores the key security challenges facing the oil and gas industry and suggests specific countermeasures from the security risk management standpoint, to mitigate risks. It also covers successful implementation strategies of recommended security solutions to optimize monetary investments. RiskWatch International proposes to follow this approach during oil and gas industry projects. Inclusion of security expertise early in the planning process will result in a better-coordinated and more cost effective approach to security.

Threats Facing the Oil and Gas Industry

Security is of paramount importance in the oil and gas industry in general, and the infrastructures of the sector in particular as petroleum products dominate current worldwide consumption.

The demand surge is expected to continue in the foreseeable future, with the International Energy Agency (IEA) projecting a more than one-third demand growth over the period to 2035 . Therefore, the safeguarding of oil and gas infrastructure from all internal and external threats becomes a top priority.

Risks related to asset damage, business interruption, human casualties and damage to properties are intrinsic to oil and gas activities. Several prominent agencies throughout the world have consistently signaled at asymmetric threats from various extremist groups. The oil and gas industry is a potentially easy target primarily because of the very nature of the products used.

The chemical properties present at the facilities attract attacks as the release of the same could have devastating impact.

The fact that stability in the industry may render the government powerful also fuels the attacks. Further, the concentration of the oil and gas industry infrastructure in limited geographic areas renders it particularly vulnerable to non-traditional threats. Also, the importance of petroleum products for the overall economic stability – domestic and international – makes the oil and gas industry an attractive option for disruption of operations.

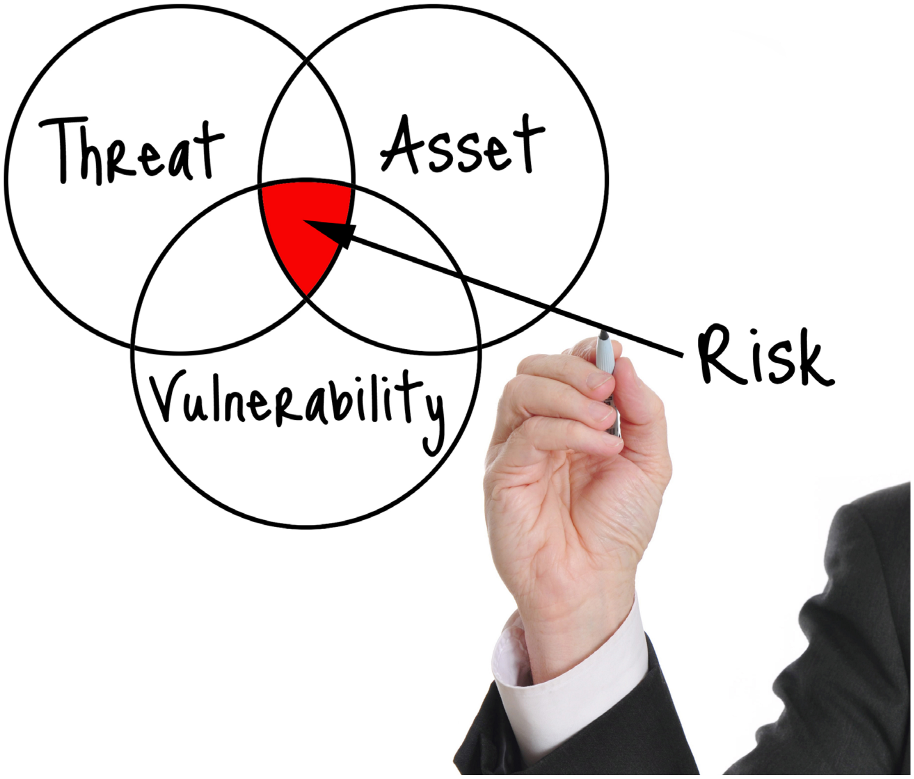
[1] IEA, World Energy Outlook 2012

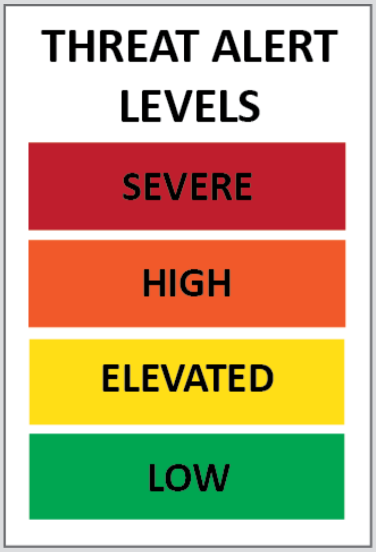
The Potential Targets: Infrastructures

While the entire oil and gas industry infrastructure is a potential target, attacks are also targeted at their strategic resources which include specific segments, equipment, support systems, transportation facilities, and technological systems. Some specific segments such as oil and gas wells, pipelines and pumping stations and storage facilities are more often located above ground in isolated areas, making them accessible for sabotage with little fear of immediate counterattack.

As a specific segment, a refinery's is vulnerable because of its urban proximity. Equipments and support systems are usually targeted to cripple local operations. Transportation systems are vulnerable because they are symbolic of the global reach of the petroleum industry.

Technological systems that companies in the oil and gas industry use are normally Supervisory Control and Data Acquisition Systems (SCADA), which are remotely controlled. Being remotely controlled renders them susceptible to malicious attacks. Also, the sector is vulnerable where it uses newer technologies that may be subject to sophisticated attacks. Therefore, as these strategic assets face unique vulnerabilities the countermeasures should also be distinctive to adapt to the security risk level.



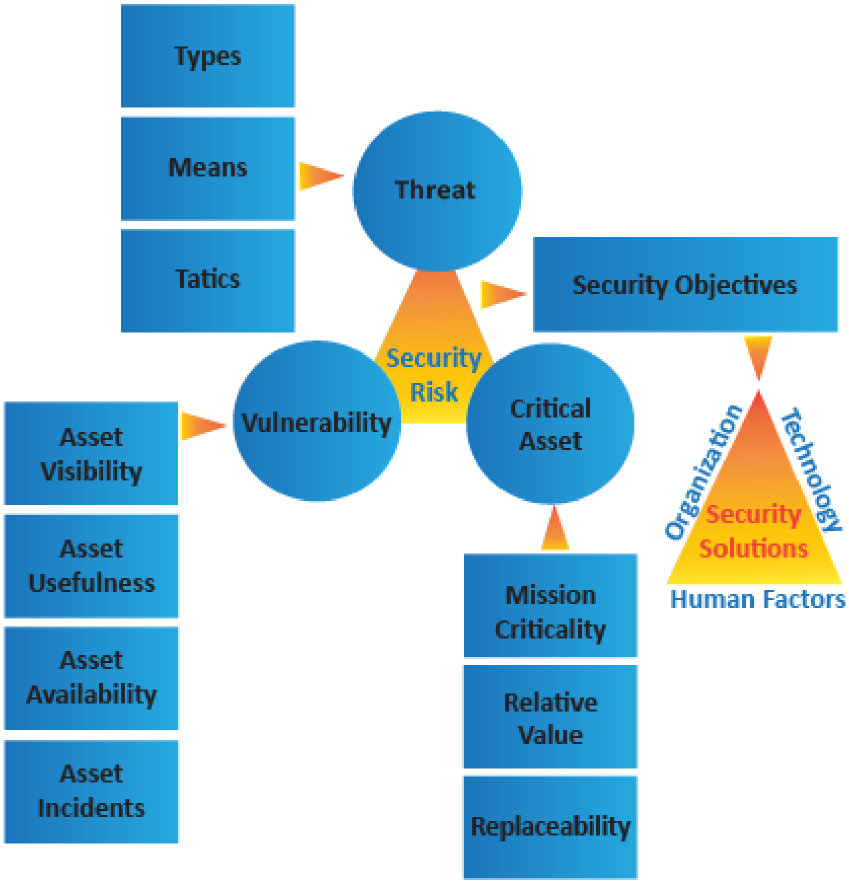


The oil and gas industry is broadly divided into various segments that cover exploration, extraction, refining and transportation. This segmentation enables terrorist groups to design varied attacks. These emerging unconventional and wider asymmetric threats coupled with the overwhelming dependence on petroleum raise serious questions about the oil and gas infrastructure protection.

Companies in the oil and gas industry face a growing number of security challenges. Their private security forces are confronting non-traditional strategy and tactics of opponents, both internal and external. The adversaries include national and international extremists, well-organized criminal syndicates, cyber security threats, ideologically driven actors, and disgruntled employees.

As the opponents and adversaries vary so do their capabilities and intentions to irrevocably damage the oil and gas industry infrastructure and thereby the heart of the economy. Their coordinated attacks can exploit the vulnerabilities inherent in protecting complex oil and gas infrastructure.

Security Risk Assessment



To counter the threats in the industry the security as well as the security risks requires a committed analysis, because the risk constitutes the threat probability and the enormity of impact on a complex resource post disaster. This is a very complex scenario that calls for desperate countermeasures. An all encompassing security risk management approach can be adopted.

The methodology will identify the security risks and assess the capabilities of the organization and its security solutions, both human and technological. While the technological assessment will include, among others, the logical, physical and environmental issues, the human solutions will cover the security forces. The security risks assessment begins once the threats, the critical assets and the vulnerabilities are ascertained and identified. It is then followed by setting of security objectives for each individual security risk that needs to be countered.

Criteria of critical representative impact include:

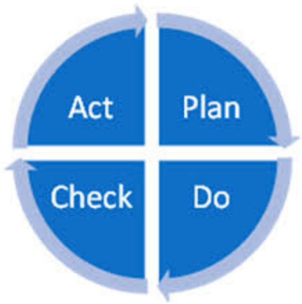
- Human casualties, killed & injured
- Economic loss of infrastructure destruction and trade disruption
- Business impact
- Civilian inconvenience due to loss of energy supply
- Environmental degradation due to hydrocarbon release
- Time loss in repair
- Potential for interdependency effects.

Comprehensive Security Risk Management

The purpose of security risk management in oil and gas is to establish a collective process to define a security program. The program enables identifying potential threats which could affect personnel, assets or operations. It also involves prioritizing those risks and identifying mitigations strategies.

In this section the white paper presents an elaborate description of the security management process to counter the potential risks and to develop a security program.

Set Up the Security Organization



Setting up the internal security organization is the first step towards initiating the risk management process. The objective of the organization is to make sure that the quality of the security management process is maintained. The internal organization will help in guiding and defining the scope and objectives of the Security Committee and the Security Working Groups.

The organization to be set up should comprise Security Committee (SC) and Security Working Groups (SWG):

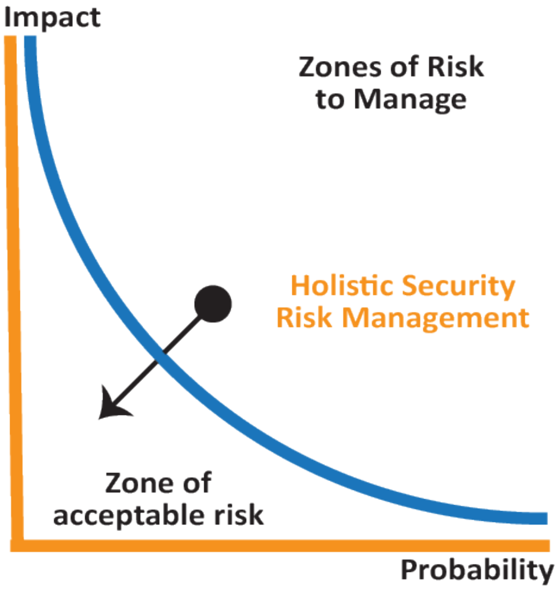
- The SC should include members from the top-level management who establish strategic and operational priorities, select courses of action, and allocate resources to develop a robust security strategy.
- The SWG on the other hand will prepare the planning documents, conduct risk assessments and develop the policy. As the SWG take on-the-ground actions, it will be positioned to recommend modifications future advancements.

The Threat WG constitutes one of the key SWGs. It comprises representatives from counterintelligence, law enforcement, information operations and the chemical, biological, radiological, nuclear, and explosives (CBRNE). Larger installations may usually incorporate additional personnel as assigned by the SC from time to time.

As stated, the security organization aims to make sure that the quality of the security management process is maintained using the Plan, Do, Check, Act (PDCA) Model.

- Plan: Establish or update the Security Master Plan (SMP) to improve security
- Do: Implement and operate the actions defined in the SMP
- Check: Monitor, review the actions and report the results to decision makers
- Act: Maintain and improve the actions

Define Security Strategy and Mitigate Risks



To mitigate the security risks the key threat areas need to be identified and duly addressed. To identify these critical threats documentation, interviews, technical review and site surveys are used. The areas that require to be addressed will include assessment of threat, criticality, vulnerability and risk.

The scope of Threat Assessment includes defining alert levels, threats identification and probability evaluation. Criticality Assessment covers identification of critical assets and defining asset criticality levels.

Vulnerability Assessment involves spotting vulnerability areas and measurement of criticality. It also covers review of manpower and security force protection. Risk Assessment provides a review to identify and evaluate the risks based on previous assessments conclusions.

Once these risks are identified, the management analyzes and takes a decision whether the particular risk should be overlooked, controlled, insured or accepted.

Implement Solutions

The security solutions should conform to the security objectives. Key security concerns focus on the protection of the critical assets. Security solutions are based on organization, human factors and technology.

If the management decides to mitigate the risk, it specifies the security objectives based on risk priority and offers solutions. The solutions are classification, detection, response and recovery.

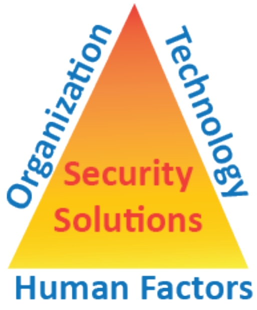
Prevention emphasizes that appropriate measures are in place to limit the probability of an incident. Detection prioritizes the implementation of detection systems and the expert monitoring of security activities. Response comprises measures that aim at analyzing alerts and follow-up response procedures. Recovery includes the measures to be taken into consideration to restore the damage. Recovery is essential to ensure the business continuity of the operations. Finally, conclusions are formalized in the SMP.

To ensure safety, organizations should implement the security solutions defined in the SMP. The implementation should constitute a series of actions covering:

- Security solutions prioritization

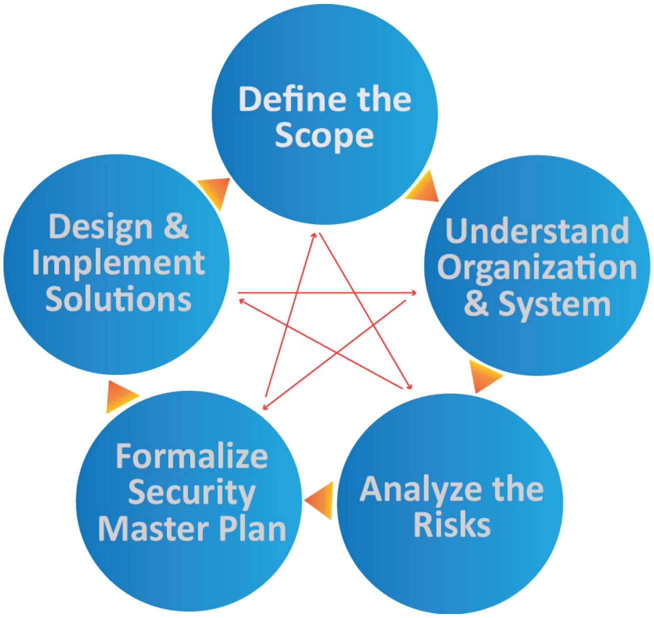
- Planning accomplishment supported by adequate funding.

Once additional countermeasures are identified and implemented, it is time to reassess the security risks. In this regard, a risk management scorecard is of immense help. Also, it is very vital to conduct complete risk assessment on yearly basis.



Pipeline Systems	🟥	🟩	🟨	🟨
Oil Refineries	🟨	🟥	🟨	🟨
Mass Storage Facilities	🟨	🟩	🟩	🟥
Reservoirs	🟥	🟩	🟩	🟩
Wells	🟩	🟩	🟩	🟩
Offshore Production Facilities	🟩	🟩	🟩	🟩

Security Management Best Practices



Define the Scope
Understand Organization & System
Analyze the Risks
Formalize Security Master Plan
Design & Implement Solutions

Decades of working along with its global oil and gas industry partners have enabled RiskWatch International to help several organizations with unmatched security solutions. With such unparalleled expertise RiskWatch has identified some best practices in the oil & gas industry security management. They include:

• Risk management: Corporates should aim at integrating a comprehensive security risk management system into the organizations overall risk management process.

• Security organization set up: To ensure that the quality of the security risk management process is maintained, create senior level security committee, SWGs, corporate security risk team and local security officers including IT, safety and facility.

• Coordination: Facilitating coordination with government and stakeholders including customers, suppliers and infrastructure providers to achieve collaborative development.

• Security Master Plan: Defining the SMP serves as a cohesive security solution and addresses all aspects of security planning simultaneously.

• Resilience management: An effective resilience management approach helps organizations manage operational risk and improve operational resilience.

• Interdependencies: Interdependencies calls for evaluation of contingency plans from an infrastructure interdependencies perspectives. It enhances coordination with industry wide infrastructure providers.

• Human resource: It has a multidimensional role to play – from ensuring background investigations and periodic updates for employees to defining a hiring policy to raising employee awareness.

• Physical security: The physical security division serves as a strategic partner in combating the growing number of challenges in the industry. It helps guard sensitive areas by restricting access, and should provide increased security checkpoints, robust manned facilities and video surveillance.

• Information System and Network architecture: As part of a robust IT security policy, organizations should specify LAN/WAN network perimeter, curtail external connections and keep up to date mapping of network. Traffic filtering, authentication controls, encryption, and access controls should be covered.

This white paper proposes a Scope Of Work that details a security strategy development which includes the best practices.

Typical RiskWatch Scope of Work

RiskWatch International has defined the Scope of Work to support oil & gas companies in developing an efficient security risk management process. As depicted in the figure below, the RiskWatch SOW involves five key components:

Step 1: Specify the Scope

RiskWatch reckons defining the scope of the Risk Management Program as the first important step and proposes:

- Meeting senior management to set up and define the SWG.
- Understanding the business objectives to formalize the scope of the System.
- Defining the scope of the System to formalize the planning of the security risk management program.

Step 2: Understand the organization and the System

As the second key step, in understanding the organization and the System RiskWatch considers:

- Understanding the organization and its System, its relations with government agencies and identifying the regulatory challenges to acquire an understanding of the context.

Step 3: Risks Assessment

Evaluating the prevailing security risks in the System constitutes the next step. In this regard RiskWatch recommends:

- A thorough review of the System, and undertaking the threat, criticality and vulnerability assessment.
- Categorization of risks to accept, to ignore, to control or to ensure, and suggesting security objectives.
- Advising security solutions to mitigate risks.
- All the above three should lead to the security risk measurement report.

Step 4: Formalize the security master plan

Based on the decisions provided by the SC and the SWG, a SMP is formalized to define the security policy and the operational concept. RiskWatch International considers the following:

- Prepare & propose implementation of security solutions, return on security investment (ROSI) calculations.
- It leads to documents concerning Security Risk Management Methodology, SMP, Security doctrine and operational concept. The output should include implementation plan report and the ROSI report.

Step 5: Devise and implement solutions

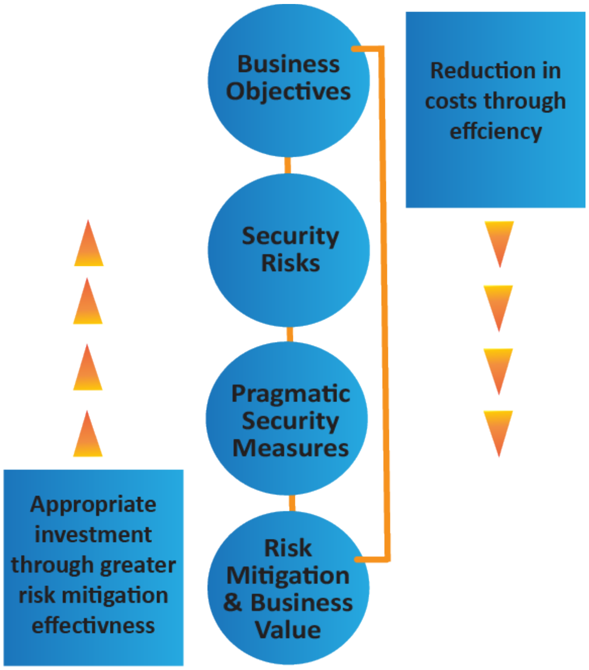
In this last step of implementing the Security Master Plan actions, Riskwatch proposes:

- Defining a new security organization including the SC and SWGs, developing operational security procedures, designing security control rooms, implementing physical security, and individual protective measures.
- Developing operational and technical training program and implementation of communications security.
- Implementing a robust information technology security solution and building particular software to generate daily scorecard of the risk condition.
- Developing effective resilience solutions to manage operational risk and improve operational resilience.
- Sustain the quality of the security solution participating in the PDCA process.
- All the above ensure that the security solutions are implemented and maintained.

The objective of the SOW is to provide a foundation for conducting risk assessments and evaluating security risk management options. To this purpose, RiskWatch International has developed Critical Asset Security Risk Management, CASRIM. CASRIM is a unique software program that assists RiskWatch engineers to fully analyze the major security risks. The software generates graphical display of the risk analysis after a careful scrutiny of the situation.

Benefits of a Comprehensive Approach

Risk assessment involves the integration of threat, vulnerability, and consequence information followed by protective measures based on an agreed upon risk mitigation strategy. Risk determination aids the management in prioritizing the protection of critical assets after relative study of the asset valuation and the probable vulnerabilities. This, in turn, helps the management in accepting the vulnerability risks. However, the management must guard against all risk exposures by building a risk management framework to prevent incident, deploy countermeasures to mitigate the incident enormity, and recuperate post incident.


Business Objectives
Security Risks
Pragmatic Security Measures
Risk Mitigation & Business Value
Reduction in costs through effciency
Appropriate investment through greater risk mitigation effectivness

Adopting a comprehensive approach enables minimal financial costs to yield sizeable benefits in cases of security solutions for already identified risks. Further, organizations gain efficiencies due to integration between the security technology, the organizations objectives and processes. All this is achieved while remaining secure throughout.

Implementation of security measures on existing structures tends to be operationally less useful than those adopted during initial infrastructure facility design. Similarly, security measures aimed at covering up a lack of initial stage planning don't always produce the desired benefits. Delays in adopting a security and control strategy could lead to a costly outcome such as network attacks, production interruptions and loss of reputation. Therefore, it is profitable to incorporate strategic security measures during initial infrastructure facility design and initial planning.

Conclusion

The oil & gas industry is subject to countless potential security breakdowns. Companies can adopt a comprehensive security risk management strategy to adapt security solutions to the emerging threats and security risks. The risk management framework will also help in balancing fund allocation on the basis of the required protection. While security for mega infrastructures should reflect financial capabilities, security projects for infrastructures with limited funding should be planned at a manageable cost.

The methodology presented in this white paper is scalable and can be adopted to measurably improve the security scenario from a single infrastructure to the entire oil and gas value chain – upstream, midstream and downstream.