Corporate Security Programs – Security Risk Management

Our security risk management process provides the flexibility needed for proactive decision making to address the security risks of corporate facilities. Security risk management activities should be commensurate with the type, size, location and criticality of the assets being protected. Using methodologies that encompass all facets of threat, vulnerability and asset characterization result in a comprehensive Corporate Security Program (CSP) designed to meet corporate needs immediately and in the long term.

Asset Characterization

All assets (people, facilities, material, information, reputation or an activity that has a positive value to the operator) shall undergo an evaluation of their criticality. Severity of consequences and asset attractiveness can be used to screen assets to identify those that require only general security countermeasures and those that require more specific security countermeasures. Using this information, assets can be prioritized based on the severity of consequences.

Corporate Security Programs- Security Risk Management

A documented process will be developed and implemented to identify any current and potential threats against corporate assets that could result in the loss or damage to an asset. The threat assessment will consider available and relevant information from both internal and external sources and be reviewed and updated at regular intervals or as circumstances dictate.

Threat Assessment

Threat assessment procedures will determine the following:

- Presence and identification of a potential adversary.
- Capability of an adversary to carry out a threat based on an assessment and evaluation of the nature of the threat and degree of sophistication needed to carry out the threat (e.g., specific training, financial support, and industry expertise).
- Intentions as to whether the threat has been stated or implied and belief that the threat is real.
- History of a similar threat having occurred in the past to another similar operation within the same industry or region.
- Specific information as to whether the threat identifies the target or the potential attractiveness of a target.
- Immediacy of the threat being carried out (e.g., date or timeline).
- Probability of the threat being carried out based on the reliability or credibility of available information.

Vulnerability Assessment

Upon completion of the threat assessment, a vulnerability assessment will identify existing safeguards or security countermeasures and determine the efficiency of those identified safeguards and countermeasures with regard to the threats presented.

Security Risk Assessment and Risk Mitigation

The combined results will enable the corporation to evaluate, prioritize and implement available countermeasures to reduce vulnerabilities or consequences. The status of corporate security in real time, coupled with assessment of all facets of the business will result in the development of mitigation strategies that need to be addressed immediately and those that need to be incorporated over time. These strategies are in accordance with a graduated risk mitigation matrix developed to meet corporate risk tolerance and increased threat profiles.

Information Security

Management Procedures and policies pertaining to information technology security and information security are often contained in the internal Information Security Policies and Procedures and shall be in accordance with CAN/CSA Z246.1-09 Security Management for Petroleum and Natural Gas Industry Systems. This includes:

- Training and awareness on information security policies and procedures.
- Classifying internal information (e.g., assigning classification levels, ranging from least to most sensitive, such as "restricted", "confidential" and "proprietary").
- Handling and storage of information commensurate with its classification level and its security risk.
- Handling of external information.
- Security clearances for individuals with designated positions.
- Records and documentation that comply with the company's security and privacy policies and procedures, including destruction.
- Information technology/control systems security.

Personnel Security

The Corporation should develop a personnel security process that addresses:

- The protection of employees and other on-site personnel.
- The roles, responsibilities and management accountability structure to ensure compliance with the corporate security policy.
- The protection measures required to provide a safe and secure workplace.

Security Awareness Training

Security Awareness Training (SAT) shall include:

- Training for employees and on-site personnel across all facilities.
- Be conducted as part of new employee orientation.
- Be provided on a regular basis.
- Be conducted in accordance with the Corporation's Human Resources Policies, such as personnel screening for those personnel who may have access to restricted areas or information, employee/on-site personnel termination policies, work alone policy, travel policies/procedures to minimize security risks and threats during business travel.
- Include development of security messages for internal communication that will promote a security culture and support the security practices.
- Operational security including:
  - » Threat environment.
  - » Surveillance techniques.
  - » Suspicious activities.
  - » Threat-level response measures and policies.
  - » Physical security measures, including access controls and security badges.
  - » Confrontation and communication training.
  - » Personal protection training.
  - » Recognition and reporting of security-related threats/incidents or information that might help detect security threats. Includes a component that tests and assesses knowledge and understanding across the organization in applying the security awareness content specific to operational requirements.
  - » Includes a relevant security stakeholder component to enhance community awareness through various communication methods.
  - » Maintains procedures to protect the integrity of training records in accordance with corporate record retention policies.