Threats to Energy Infrastructure

- Accidents
- Vandalism
- Severe Weather
- Random Equipment Failures
- Power Outages
- Cyber Attacks
- Terrorist Attacks
- Disruptions in Financial Markets
- Financial Failure of Counter Parties
### Vulnerability Assessment Framework

<table>
<thead>
<tr>
<th>Initiating Events</th>
<th>Protective Measures</th>
<th>Critical Assets</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe Weather</td>
<td>Physical Security</td>
<td>Physical Plant</td>
<td>No Impact</td>
</tr>
<tr>
<td>Cyber Attack</td>
<td>Cyber Security</td>
<td>Employees</td>
<td>Loss of Revenue</td>
</tr>
<tr>
<td>Accident</td>
<td>Safety Systems</td>
<td>Brand/Reputation</td>
<td>Loss of Production</td>
</tr>
<tr>
<td>Disruptive Financial Event</td>
<td>Training</td>
<td>Business Capability</td>
<td>Capability</td>
</tr>
<tr>
<td>Terrorist Attack</td>
<td>Contingency Plans</td>
<td>Critical Info/Processes</td>
<td>Decline in Stock Price</td>
</tr>
<tr>
<td>Power Outage</td>
<td>Insurance</td>
<td>IT Resources</td>
<td>Loss of Reputation</td>
</tr>
<tr>
<td></td>
<td>Emergency Response Plans</td>
<td>Financial Resources</td>
<td>Death/Injury</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bankruptcy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Demise of Enterprise</td>
</tr>
</tbody>
</table>
Enterprise Risk Management (ERM)

- Assess vulnerabilities to all events of concern on a common basis.
- Consider all assets that can be impacted by the events/threats.
- Develop risk measures for each asset-event combination.
- Develop a comprehensive risk management program to address significant vulnerabilities.
- Allocate protection resources to match risks.
Risk Definition

The Risk to an asset from a particular event or threat is defined as:

\[
\text{Risk} = \text{Likelihood the Event Occurs} \times \text{Likelihood that the Asset is Impacted by the Event} \times \text{Consequences of the Impact}
\]
Consequence Estimates

• Consequences may be very different for different types of assets.

• The key to comparative risk assessment is to develop qualitative measures that put consequences on the same relative scale, such as:
  – Unacceptable
  – Critical
  – Undesirable
  – Nuisance
Likelihood Estimates

• Quantitative estimates of the likelihood of many events (e.g., terrorist attack) are not available
  – Likelihood of occurrence is not known
  – Likelihood of impact on assets is at best difficult to quantify

• Qualitative likelihood estimates can be developed for essentially any event
  – Very High
  – High
  – Moderate
  – Low
**Risk Matrix**

Risk Level (High-Red, Moderate-Yellow, Low-Green) for Impact-Likelihood Combinations

<table>
<thead>
<tr>
<th>Likelihood Asset is Impacted</th>
<th>Impacts of Events on Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unacceptable</td>
</tr>
<tr>
<td>Very High</td>
<td>H</td>
</tr>
<tr>
<td>High</td>
<td>H</td>
</tr>
<tr>
<td>Moderate</td>
<td>M</td>
</tr>
<tr>
<td>Low</td>
<td>M</td>
</tr>
</tbody>
</table>
Summary

• Our energy infrastructure is vulnerable to many types of events.
• Enterprises have difficulty comparing risks from different events and allocating protection resources.
• Managers are under increasing pressure to verify that prudent protection measures are in place.
• ERM provides managers the tools they need for comprehensive risk management programs.
  – Risk Identification
  – Risk Assessment
  – Risk Resolution