Agenda

- Introductions
- What Brought Us Here
- Utility Industry Observations
- Approach and Management of CIP-014
  - Threat and Vulnerability Assessments
  - Developing Mitigation Options
- Collaborative Approach to Physical Security
  - Mitigation Implementation
- Questions
Background

► PG&E’s Metcalf – April 16, 2013
► Mainstream Press
  • Wall Street Journal
  • USA Today
► Media Drives Industry
► March 7, 2014 – FERC Directs NERC (ERO)

"Destroy nine interconnection substations and a transformer manufacturer and the entire United States grid would be down for at least 18 months, probably longer," said the memo, which was reviewed by the Journal.


The attack was "the most significant incident of domestic terrorism involving the grid that has ever occurred" in the U.S., said Jon Wellinghoff, who was chairman of the Federal Energy Regulatory Commission at the time.

- Wall Street Journal, Feb. 4, 2014
Additional Notable Events

- **October/November 2015** Kershaw County, SC
- **October 2015** Edmonton, Canada
- **November 2015** Erie, Pa
- **April 2014** Newfoundland, Canada
- **August 2013** Lake Placid, FL
- **September 2012** Tahlequah, OK
- **March 2015** Bakersfield, CA
  - First Night – 2 people spotted at 4 a.m., contract security call local PD
  - Damaged Transformer by cutting wires
  - Second Night – cut in through same hole
    - Breached control shelter, powered down equipment, cutting cords
Why Does This Matter

- 2 Events Increase Security Spending
  - Ink on Paper – Regulation
  - Blood on Pavement – An Event
- Utilization of Insurgency Tactics
- Demonstrated
  - Preoperational Surveillance
  - Preoperational Planning
  - Detailed Target Selection
- Infrastructure – Water/Power
  - Soft Targets
  - Societal Reliance
- Leading Indicator of Dynamic Threat Shift?
Approach and Management of CIP-014
Industry Observations

- Utilities Being Active
  - CIP-014 Sites
  - “Company Critical” Sites
- NERC CIP-014 & Security Programs
- Prescriptive vs. Nonprescriptive
- Uncertainty of Minimums
- “Security” Firms Emerging
- Writing “The Story”
Conducting the Threat Assessment

- **Terminology**
  - Threat – who the bad guy is
  - Risk – what the bad guy could do
  - Vulnerability – how the bad guy can do it
Conducting the Threat Assessment

Based on Source Data

- Federal Government (U.S. and Canada)
- Provincial Government
- Local Law Enforcement
- Utility-specific Incident Reports
- Utility-wide Incidents
Conducting the Threat Assessment

- Threat Assessment **IS**
  - Information to Guide Vulnerability Assessment
  - Information to Guide Adversary Assumptions
  - A Snapshot of Time
  - Perishable

- Threat Assessment **IS NOT**
  - Static
  - A Detailed List
  - Does Not Address Probability of Event
Conducting the Vulnerability Assessment
Conducting the Vulnerability Assessment

- Thinking Like the Adversary
  - Understanding the Attack Model
    - Event Selection
    - Target Selection
    - Preoperational Surveillance
    - Attack Mobilization
    - Attack Dry Runs
    - Attack Sequence

- Nuclear Security vs. Substation Security
Vulnerability Assessment

- Define the Adversary
  - Complex – Asset Shooting
  - Basic – Copper Theft
- Measure Site in Relation to Adversary Risks
  - Copper Theft
  - Trespass
  - Asset Shooting
  - Improvised Explosive Device
  - etc.
Risk Assumptions Sample 1

- **Asset Theft**: the unauthorized removal of facility assets.

  - **Assumptions:**
    - Adversary desires to remove the assets while minimizing potential detection or evidence that would lead to apprehension.
    - Assets subject to theft are to be both man portable spools and large truck transported spools of high value commodities, such as copper.
    - Motivation for asset theft events is not driven by a desire to harm a facility, but rather to acquire the asset components being removed.
      (Harm to the facility and operation can occur based on the type(s) of assets stolen and the downtime associated with asset replacement.)
Vulnerability Assessment

- Thinking Like the Adversary
  - Attack Considerations
    - Target Attractiveness
    - Ease of Attack – Success/Vulnerability
    - Likelihood of Attack
  - Adversary Attack Routes
  - Terrain
  - Population Densities
  - Identifying Pros and Cons
## Vulnerability Analysis

<table>
<thead>
<tr>
<th>Target Attractiveness</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
</tr>
<tr>
<td>Low</td>
<td>2</td>
</tr>
<tr>
<td>Very Low</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Likelihood of Event</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>81-100</td>
</tr>
<tr>
<td>High</td>
<td>61-80</td>
</tr>
<tr>
<td>Medium</td>
<td>41-60</td>
</tr>
<tr>
<td>Low</td>
<td>21-40</td>
</tr>
<tr>
<td>Very Low</td>
<td>0-20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>0.8</td>
</tr>
<tr>
<td>High</td>
<td>0.6</td>
</tr>
<tr>
<td>Medium</td>
<td>0.4</td>
</tr>
<tr>
<td>Low</td>
<td>0.2</td>
</tr>
</tbody>
</table>
## Vulnerability Analysis

<table>
<thead>
<tr>
<th>Sample Site 1</th>
<th>Likelihood of Event</th>
<th>Facility Attractiveness</th>
<th>Scenario Likelihood</th>
<th>Likelihood of Success</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forced Entry (Electric)</td>
<td>90</td>
<td>1</td>
<td>90</td>
<td>0.4</td>
<td>36</td>
</tr>
<tr>
<td>Theft (Electric)</td>
<td>100</td>
<td>1</td>
<td>100</td>
<td>0.2</td>
<td>20</td>
</tr>
<tr>
<td>Small Arms</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>0.2</td>
<td>2</td>
</tr>
<tr>
<td>Sabotage</td>
<td>8</td>
<td>3</td>
<td>24</td>
<td>0.8</td>
<td>4</td>
</tr>
<tr>
<td>VBIED</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>0.8</td>
<td>4</td>
</tr>
<tr>
<td>Coordinated</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>0.8</td>
<td>4</td>
</tr>
<tr>
<td>Standoff</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>0.6</td>
<td>3</td>
</tr>
<tr>
<td>Explosive</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>0.2</td>
<td>0.6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sample Site 2</th>
<th>Likelihood of Event</th>
<th>Facility Attractiveness</th>
<th>Scenario Likelihood</th>
<th>Likelihood of Success</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forced Entry (Electric)</td>
<td>90</td>
<td>1</td>
<td>270</td>
<td>0.6</td>
<td>162</td>
</tr>
<tr>
<td>Theft (Electric)</td>
<td>100</td>
<td>2</td>
<td>200</td>
<td>0.4</td>
<td>80</td>
</tr>
<tr>
<td>Small Arms</td>
<td>10</td>
<td>5</td>
<td>50</td>
<td>0.8</td>
<td>40</td>
</tr>
<tr>
<td>Sabotage</td>
<td>8</td>
<td>3</td>
<td>24</td>
<td>0.2</td>
<td>4.8</td>
</tr>
<tr>
<td>VBIED</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>0.8</td>
<td>4</td>
</tr>
<tr>
<td>Coordinated</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>0.8</td>
<td>4</td>
</tr>
<tr>
<td>Standoff</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>0.6</td>
<td>3</td>
</tr>
<tr>
<td>Explosive</td>
<td>3</td>
<td>2</td>
<td>6</td>
<td>0.4</td>
<td>2.4</td>
</tr>
</tbody>
</table>
An Effective Security Plan

► Deter – Target Shifting
  • Lighting, signs and physical changes
► Detect – Identify Adversary
  • Intrusion detection and cameras
► Delay – Slow Access
  • Anti-rams devices, enhanced/secondary fences, asset barriers
► Respond – Documented Protocols for Owner and Law Enforcement
Defining Mitigation Strategy

- Devaluing the Target
  - Target Shift
  - Method Shift
- Deterrence Model
- Detection Model
- Peanut Butter Approach
- Develop Assumptions of Risks
  - Assessment without Assumptions
Defining Mitigation

- Based on:
  - Site Constraints – Rural vs. Urban
  - Industry Trends
  - Project Experience
  - Operational Tempo
  - Congruent with Security Strategy
  - Environmental Considerations
  - Proven Technologies
Mitigation Selection – Utility Considerations

- Security Officers
  - Cost
  - Observe and Report vs. Intervention
  - Liability Issues
  - Adversary Action

- SOC Personnel
  - Defining Response
  - System & Team Capabilities
  - Response CANNOT Start Until Detection
Mitigation Selection – Utility Considerations

- Cameras
  - Pros/Cons
    - Thermal
    - IR Illuminated
    - Visual Trespass
    - Over Abundance
    - Maintenance and Testing
Mitigation Selection – Utility Considerations

- Intrusion Detection
- Long Range Detection
  - Pros/Cons
    - Nuisance Alarms
    - Native Animals
    - Terrain
    - Maintenance and Testing
Mitigation Selection – Utility Considerations

- Fencing/Barrier Options
  - Pros/Cons
    - Walling Effect
    - Vegetation
    - Visibility
Mitigation Selection – Utility Considerations

- T-Walls/Ballistic Barriers
  - Pros/Cons
    - Ballistic?
    - Cost/Benefit
    - Visibility
Mitigation Selection – Consolidated Approach
Implementation Considerations
Successful Corporate Structure

- Identify Departments & Accountability
  - Assign Ownership to Single Group
  - Assign Task Manager from Each Department
  - Compliance & Support from Top Down

![Diagram showing a corporate structure with PM at the top, Dept 1 and Dept 2, and Team 1, Team 2, and Team 3 below.]

[Image 11x17 to 781x595]
Collaborative Approach

- **Security** Planning & Technologies
- **Engineering** Considerations
- **Permitting**, Real Estate and the Public
- And Everybody Else

Substation Security Program

- Transmission Engineering
- Substation Engineering
- Corporate Security
- Permitting and Real Estate
- Construction
- Information Technology
- Distribution Engineering
Engineering Considerations

Surveys and Line of Sight

- OH (LiDAR), UG, & Topo
  - LiDAR for LOS & Clearances
  - Obstruction Mitigation
  - Permitting Requirements
  - Manufacturing Accuracy

- LOS
  - Determine Exposure
  - Perimeter vs. Asset
Engineering Considerations

Asset Barriers
- Primarily Enclosures & Transformers
- Ballistic Protection
  - Based on LOS
  - UL 752
- De-rating Concern
- Clearances
- Maintenance

Ballistic Protection: physically securing substations.
Engineering Considerations

Hardened Fence
- Perimeter Barriers
- K-Rated Gates
- Ballistic Protection
- Access Control
- Geotech Reports
- Electrical Clearances
  - Clearance Reports
- UG Obstructions
- Site Drainage
Engineering Considerations

Technology & Station Service
- Coordination w/ Security
  - Internal & External
- Power Analysis
  - Independent
  - Uprate
- Bandwidth (IT)
  - Leased Lines
- Telco Relocation
Engineering Considerations

Grounding

- **Powder Coating**
- Panels & Posts
- Gates & Moving Parts
- Develop Standards
  - Manufacturer Solutions
Construction, Operations & Maintenance

- Construction
  - Survey Staking
  - E&S Controls
  - Temporary Fencing

- Operations & Maintenance
  - Ingress & Egress
    - Card Scanners
    - Internal Gate Opening
  - Motorized (Roll-ups)
  - Culverts
Permitting, Real Estate and the Public

- Assess the Needed Permits Immediately
  - Local
  - State/Provincial
  - Federal

- Rights and Restrictions of Current Site
  - Security Design Changes
  - Frequent Communication with Construction

- Future Needs at Site
  - Maintain Relationships
Permitting, Real Estate and the Public

▶ Common Requirements
  • Site Plan Amendments
  • Land Disturbance
  • Building Permits
  • Conditional Use Permits

▶ Construction Limitations
  • Linear Feet – Disturbed Earth
  • Dusk-to-Dawn Lighting

▶ Constant Communication
Timing is Everything

Meeting Must be Scheduled
- Local law enforcement
- Neighbors
- Public officials

Develop a Plan
- Level and means of communication
- Consistent messaging

*What do you know that we should know??????*
Anticipate Reaction

▶ Privacy Concerns
  • Cameras, motion sensors and lighting
  • Sound “gun shot” detectors

▶ Physical Changes
  • Fence heights or coloration
  • Drainage changes
  • Landscape removal
Questions

Robert J. Hope, CPP
Manager – Security Consulting
Burns & McDonnell Engineering
816-349-6754
rjhope@burnsmcd.com