Overview

• Substation Incidents
• NERC CIP-014
• Substation Solutions
• What about Cyber
Substation Incidents

1990 - Lake Placid-area power transformer that shot up by a man armed with an AK-47. In 1993, persons unknown fired 50 to 100 rounds into the same substation using multiple weapons.

1990 - City of Broken Bow, Okla. Three men fired into a local substation, then slashed tires of police cars in apparent planning for a robbery spree.

1994 - Florida deputies narrowly avoided being sprayed with semiautomatic fire from a fleeing van when they responded to a shooting that damaged a Tampa Electric substation.

2006 - Two South Dakota men were arrested for shooting up a transformer near the town of Sisseton and likely were behind a string of attacks dating back to 2001.

2013 - Vermont's Barton Village spent $250,000 last year replacing a transformer damaged by gunfire.
Substation Incidents

April 2013 – In California, “snipers” targeted 17 power transforms that funnel power to the silicon valley. It took 27 days to bring the station back on line. Then in Aug 2014 Intruders cut through fences and stole $38,000 of tools and equipment.

February 2014 - In Arizona, shooters were seen on the footage of a security camera, they dispersed before police could arrive on scene.

June 2014 - In Arizona, a bomb was found next to a substation’s diesel tank, the threat was averted.
 Shots in the Dark
A look at the April 16 attack on PG&E’s Metcalf Transmission Substation

1. 12:58 a.m., 1:07 a.m. Attacker cut telephone cables
2. 1:31 a.m. Attacker open fire on substation
3. 1:41 a.m. First 911 call from power plant operator
4. 1:45 a.m. Transformers all over the substation start crashing
5. 1:50 a.m. Attack ends and gunmen leave
6. 1:51 a.m. Police arrive but can’t enter the locked substation
7. 3:15 a.m. Utility electrician arrives
Metcalf has become both a warning and an obsession, the subject of numerous talks at industry conferences. But John Lightfoot, who manages the FBI's counterterrorism efforts in the Bay Area, says much of the public discussion of the incident has been wrong.

"We don't think this was a sophisticated attack," said "It doesn't take a very high degree of training or access to technology to carry out this attack."

One shooter likely – gunshots, their flash captured on a security camera video, show only one rifle firing at a time. "That indicates to us that there was only one shooter,"

Not a good shot - "This guy was standing 60 yards away from a target the size of a house, and we didn't find as many bullet holes as we found rounds, which means that at least some of the rounds completely missed the target."
So What?

Not Terrorism,
Not Sophisticated,
Not a good shot,
Intent was not terrorism,
Single shooter...

It amounts to the same thing, might even make it worse.
CIP-014-1

Adopted in May 2014
Enforcement Date Oct 1, 2015

Requirements:
• Risk assessment by owners
• Threat evaluation against physical attack
• Develop and implement security plan
Requirement R1: Stipulates that each Transmission Owner is to perform an initial risk assessment on those transmission stations and substations that meet the applicability criteria. This risk assessment is for the purpose of identifying any facilities that if “rendered inoperable or damaged could result in widespread instability, uncontrolled separation or cascading within an interconnection”. The draft calls for subsequent risk assessments on a defined schedule depending on the results of the initial analysis.
Requirement R2: Requirement R2 calls for unaffiliated third-party verification of the risk analyses performed in fulfillment of R1. The standard allows this third-party verification to occur simultaneously with the initial risk assessment or be conducted subsequent to completion of the assessment. Section 2.4 of R2 also calls for each transmission owner to develop procedures to protect the confidential risk assessment information provided to and received from the third-party verification entity.
Requirement R3: Requirement R3 calls for transmission owners with facilities that have been identified and verified according to Requirements R1 and R2, but are not under the operational control of the transmission owner, to notify the transmission operator of these facilities of their identification under R1 and verification under R2.
CIP-014-1

Requirement R4: Requirement R4 calls for transmission owners with facilities identified in R1 and verified in R2 to “conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s)”.
Requirement R5: Requirement R5 calls for each transmission owner with facilities identified in R1 and verified in R2 to “develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s)”. The content of these plans is to include measures to deter, detect, delay, assess, communicate and respond to potential physical threats and vulnerabilities. Law enforcement coordination is also to be addressed.
CIP-014-1

Requirement R6: Requirement R6 calls for the independent verification of the security plans developed in R5. Section 6.1 of R6 states that this third-party review entity must have at least one member holding either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification both of which are promulgated by ASIS International. Other third-party review options include an entity or organization approved by the ERO, a governmental agency with physical security expertise or an entity with demonstrated law enforcement, government or military physical security expertise.
Risk

- Risk = (Likelihood of Event) * (Severity of Consequences)

- Consequences tends to be defined in terms of:
  - Dollars
  - Lives
  - Reputation loss
  - Lost opportunity
Substation Protection

Transformers can be shielded from public view using bullet proof barriers. Although barriers must be designed to permit adequate ventilation for cooling and be either moveable or positioned so as to allow transformer maintenance and eventual replacement, neither of these design considerations are difficult or expensive to implement.

“...crash resistant fences and a concrete wall would add perhaps $100,000 to $200,000, a few percent of the multi-million dollar facility cost.” [1]

Substation Protection

Line of site deterrent such as a cinder block wall
  o Surrounding terrain

Highest value assets enclosed in a ballistic barrier
  o Maintenance and Access
  o Minimum distance for airflow under worst case situations

CCTV and video analytics
  o Lighting restrictions
  o Response time / Location
Thermal Cameras

- Significantly reduced pricing
- No lighting required
- Low resolution - best for analytics and reducing false alarms
- Visible and thermal - dual units for tracking and identification
Video Analytics

• Combines detection and assessment functions
• Works best in a controlled (i.e. interior) environment
• Significant progress for exterior applications
• License plate analytics
• Manufacturers are embedding analytics at the camera edge for more efficiency
Thermal and Visible CCTV

Alarm Reactive and Tracking
Complementary Measures

• No single measure
• Effective design
• Expanded area of vegetation control
• More frequent security patrols
• Cooperation with local law enforcement
• Advanced video analytics
• Intrusion Detection
Cyber Events

- Home Depot
- Bank of America
- JP Morgan Chase
- Healthcare.gov
- Target
Cyber Security Controls

- Cyber Security Program Management
- Cyber Security Policies and Procedures
- Third Party Access and Outsourced Information Processing
- Asset Classification and Control
- Personnel Training and Awareness
- Incident Management
- Malware Prevention
- System Configurations
- Network Management
- User Account Management
- Physical And Environmental Security
- Business Continuity and Disaster Recovery
Program Elements

**Manage** – Activities that facilitate the management and design of processes or controls

**Monitor** – Activities that provide the ability for organizations to monitor setting and controls

**Assess** – Activities that assess the design or effectiveness of cyber security controls or processes
Program Elements - Manage

• System and Process Design
  - Policy and procedure review, design, and documentation
  - Servers, PC, Network devices configuration standards design and implementation
  - Log event alerting design
  - Define Key Performance Indicators

• Regulatory Compliance Assistance
  - Often have experience with regulators
  - Understand changes and implications
  - PCI, NERC CIP, HIPAA

• Training and Awareness Program Assistance
Program Elements - Monitor

• Network Monitoring / Intrusion Detection / System Log and Event Monitoring
  - Requires calibration
  - Requires Incident Management process

• Manage Cyber Security and Risk Management Program
  - Prioritization
  - Risk assessment
  - Monitoring and reporting Key Performance Indicators

• Configuration Benchmarking
  - Servers
  - PCs
  - Network Devices

• Helpdesk Services
  - Event log alerting
  - Vulnerability Analysis
  - Manage Incident Management program
Program Elements - Assess

• Risk Assessment / Gap Analysis
  - Tests design, not effectiveness
  - Prioritizes improvements
  - Assumes IT staff is knowledgeable and honest

• System and Network Review
  - System configuration assessment
  - Network / Firewall design assessment

• Penetration Testing
  - Adversarial approach
  - Usually use automated tools

• Social Engineering Testing
  - Tests effectiveness of awareness program
  - Important part of a continued program

• Vulnerability Scanning
  - Unauthenticated – (Pen Test)
  - Authenticated – Best Option
  - Reports on unapplied patches and upgrades
  - Used to support patch management process
Configuration Benchmarking

• Provide a custom, detailed framework for configuring and evaluating the configuration of target systems
• Consensus Configurations
  – Operating Systems
  – Databases
  – Mobile Devices
  – Network Equipment
• Recommendations for Security, Examples:
  – Ensure Firewall is Enabled
  – Logging
  – Password Settings
Questions