Corporate Risk®

>>>>>>SOLUTIONS

Protecting Critical Electrical Distribution Infrastructure

June 21, 2017

Corporate Risk® SOLUTIONS

Harford Field, III, CPP, PSP, CHS-IV

Manager, Consulting Services

Education/Training

Degree	University
Master of Arts in International Affairs (US foreign policy and international terrorism)	University of North Georgia
Bachelors of Science in Business and Public Administration (marketing and finance)	University of Texas at Dallas
Associate in Applied Science (electronics technology)	Community College of the Air Force
Certifications & Training	**Agency/Organization**
ASIS Certified Protection Professional (CPP)	ASIS International
ASIS Certified Physical Security Professional (PSP)	ASIS International
Certified in Homeland Security Level IV (CHS-IV)	American Board for Certification in Homeland Security (ABCHS)
Chemical-terrorism Vulnerability Information (CVI) authorized	Department of Homeland Security (CFATS)
Management, Leadership and Project Management	American Management Association
Electronic Warfare Systems Technology	US Air Force
Member, InfraGuard Security Network®	InfraGuard/FBI

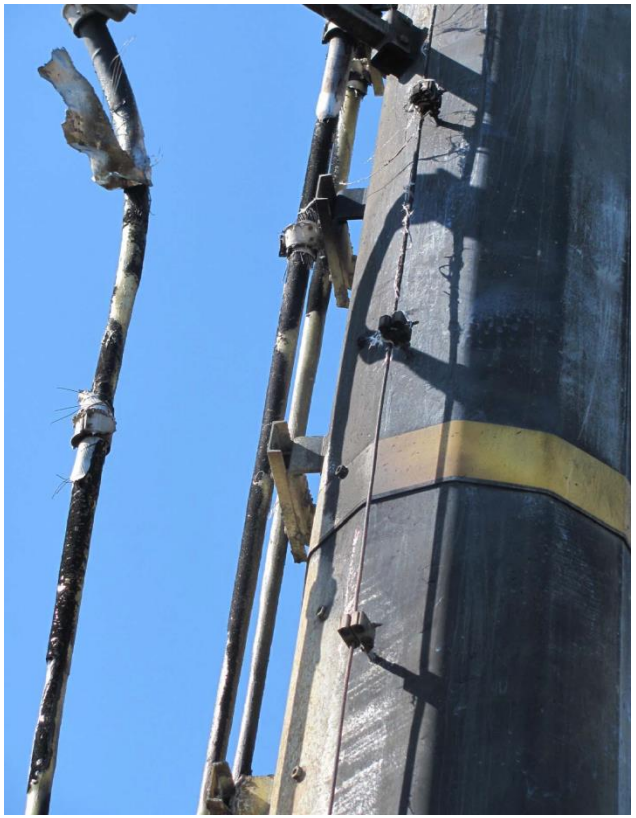
Specialties

- Perimeter security and anti-ram vehicle solutions
- Intrusion Detection Systems
- Access Control and Checkpoint Systems
- Multi-disciplinary Project Management
- Strategic Planning
- Security Site Assessments

Corporate Risk® SOLUTIONS

What's the Big Picture?

- **Vandalism?** – In 2011, an intruder gained access to a critical hydro-electric converter station in Vermont by smashing open a door lock without detection.
- **Thieves**? – In March 2013, an observed intruder climbing into Jacksonville, FL St. Johns River Power Park (coal plant) scrambled away, but was observed again attempting entry into another facility.
- **Attacks?** – Metcalf substation (a transmission sub) attacked with long-gun in 2013 driver for this workshop.

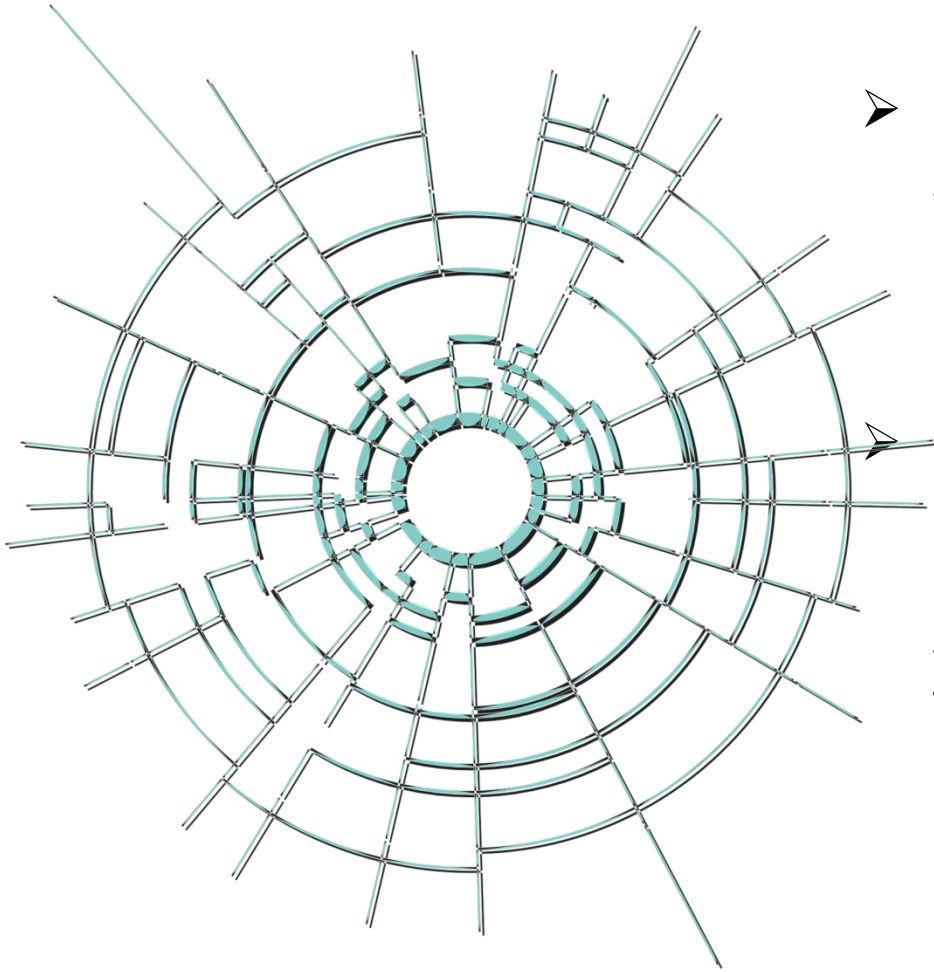


About once every four days, part of the nation's power grid – a system whose failure could leave millions in the dark – is struck by a cyber or physical attack, a USA TODAY analysis of federal energy records finds.

Corporate Enterprise Security, Inc.

Corporate Risk® SOLUTIONS

What's the Big Picture?



- **Long-gun attacks** – In 2013, multiple gunshots were fired at a gas turbine power plant along the Missouri-Kansas border and no suspects were identified.
- **Lone Wolf attacks** – Jason Woodring downs 500KV power line causing $550,000 in damage near Cabot, Arkansas in August 2013. He wanted to cut power that fed the informational downfall of America. (source: FBI)

"It's one of those things: One is too many, so that's why we have to pay attention," said Federal Energy Regulatory Commission Chairman Cheryl LaFleur. "The threats continue to evolve, and we have to continue to evolve as well." –USA Today, March 2015

Corporate Risk® SOLUTIONS

What's the Bigger Picture?

- The Metcalf Attack in 2013 was the catalyst for NERC developing a physical security standard to reduce the impact of attacks on the Bulk Electric System (BES) and provided the impetus for CA SB699 resulting in R1506009 and this workshop.
- The driver is a fear of coordinated terrorist attack(s) by domestic or international groups, especially Al-Qaeda or ISIL directed or inspired affecting the BES.
- Coordinated attacks across a broad front are expected to target taking down the electric grid which distribution systems will not cause.
- Awareness of coordinated attacks in real time is necessary to thwart such attacks. Rapid assessment and communication to authorities and other utilities is a key element. Early alerts will minimize distribution damage.

"ISIL is beginning to perpetrate cyberattacks," Caitlin Durkovich, assistant secretary for infrastructure protection at the Department of Homeland Security, told company executives at a 2015 conference of American energy firms.

Corporate Risk® SOLUTIONS

Are These Threats Real?

- Most coordinated attacks known today are cyber attacks
  - American utilities reported 13 different cyber attacks between 2011 and 2014.
  - A FOIA request revealed that the Department of Energy computer system was targeted 1,131 times between 2011 and 2014.
  - The December 23, 2015, a cyber attack on Ukraine shut down power to 700,000 homes for several hours. The event was widely blamed on the use of Black Energy malware, perhaps by Russia.
  - We now know it was a combination of denial of communications services and malware and actual damage was minimal.
  - Electromagnetic pulse or EMP is greatest threat to national grid

"Cyber attacks are often treated as a problem of technology, but they originate with human actors who employ imagination and surprise to defeat the security in place," said Tom Bolt, director of performance management at Lloyd's.

Corporate Risk® SOLUTIONS

Are These Threats Real?

- Physical attacks are less frequent and have not displayed coordination.
  - Barton Village, VT spent $250,000 replacing a transformer damaged by gunfire.
  - In 1997, an intruder entered a key substation in San Francisco, CA, throwing 39 control switches, shutting the substation down, and causing the loss of power to 125,000 for 3.5 hours.
  - A pipe bomb was attached to a transformer near Lubbock, TX and drained coolant, causing a meltdown. The intruder negotiated an 8-foot fence topped with barbed wire, the only deterrent.

"It is only a matter of the 'when,' not the 'if'—we're going to see a nation-state, group, or actor engage in destructive behavior against critical infrastructure in the United States," Rogers, who is also director of the National Security Agency, said in a speech March 2.

Corporate Risk® SOLUTIONS

What are the Consequences?

- Consequences can affect you in various ways:
  - Dollars – cost of replacement equipment, lost revenue, labor and opportunity
  - Lives – intruders can put at risk employees, customers, and first responders
  - Reputation – customers, regulators, state and federal agencies, investors, and the press
- PG&E spent an estimated $100,000,000 at its facilities in response to the Metcalf Substation incidents (yes, there were two separate incidents).
- Embarrassment of being an outlier or outside the norm in the industry, possibly spending "Metcalf" level funds.
- Criminal activity continues to drain funds and resources.

…the California substation attack, in which snipers destroyed 17 transformers, "demonstrates that it does not require sophistication to do significant damage to the U.S. grid," according to FERC. - www.utilitydrive.com, March 24, 2014

Corporate Risk® SOLUTIONS

CIP-014 Threat Definition (CTD)

- DHS moniker is DBT – Design Basis Threat
- Defines the threats and threat vectors
- NERC and NATF recommend mitigations for long-gun, vehicle-borne IED (VBIED) and personnel-borne IED (PBIED)
- FBI indicates top IED problem to be pipe bombs, not vehicles
- Focus should be on perimeter outward to deter, detect, and delay before a perimeter breach and enhanced LLE response

Primary Threats to consider include:

- High-powered Rifle (supersonic), UL Level 8 or 10
- VBIED - Vehicle-born Improvised Explosive Device (M30)
- PBIED - Persons Carrying an IED (back-pack, briefcase, box, valise) with up to 50lbs of TNT & 1,850ft stand-off
- Additional focus of insider collaboration w/above or clandestine control room takeover

* Source: NERC CIP-014-2 Physical Security Reliability Standard, March 2015

Corporate Risk® SOLUTIONS

Threat Definition for Distribution

- Theft & Vandalism - catastrophic affect to community is minimal so crime prevention is paramount
- Focus on power loss to critical infrastructure during disasters
- FBI indicates top IED problem to be pipe bombs, not vehicles though drones are rising as threat
- Early Warning - perimeter outward to deter, detect, and delay to get early response by local law enforcement

Primary Threats to consider include:

- High-powered Rifles (ala Metcalf)
- Drones able to carry 5lbs or more of explosives (growing)
- PBIED - Persons Carrying an IED (back-pack, briefcase, box, valise, pipe bomb), typically 5lbs TNT & 1,200ft stand-off
- Theft & vandalism prevention (10' anti-cut fencing, lighting, thermal PTZ where feasible, temporary motion sensors)

* Source: NERC CIP-014-2 Physical Security Reliability Standard, March 2015

Reference Guiding Authorities

- NATF has become a major influence in compliance design for security design consistency across Registered Entities and Regional Entities
- Utilize NIPP, FEMA, FBI & Fusion Centers of California
- Consult other standards such as Army FM 3-19.30
- Work with state & local law enforcement agencies
- NERC/WECC can provide additional recommendations
- Talk with other utilities & CPUC to coordinate efforts

Additional Considerations

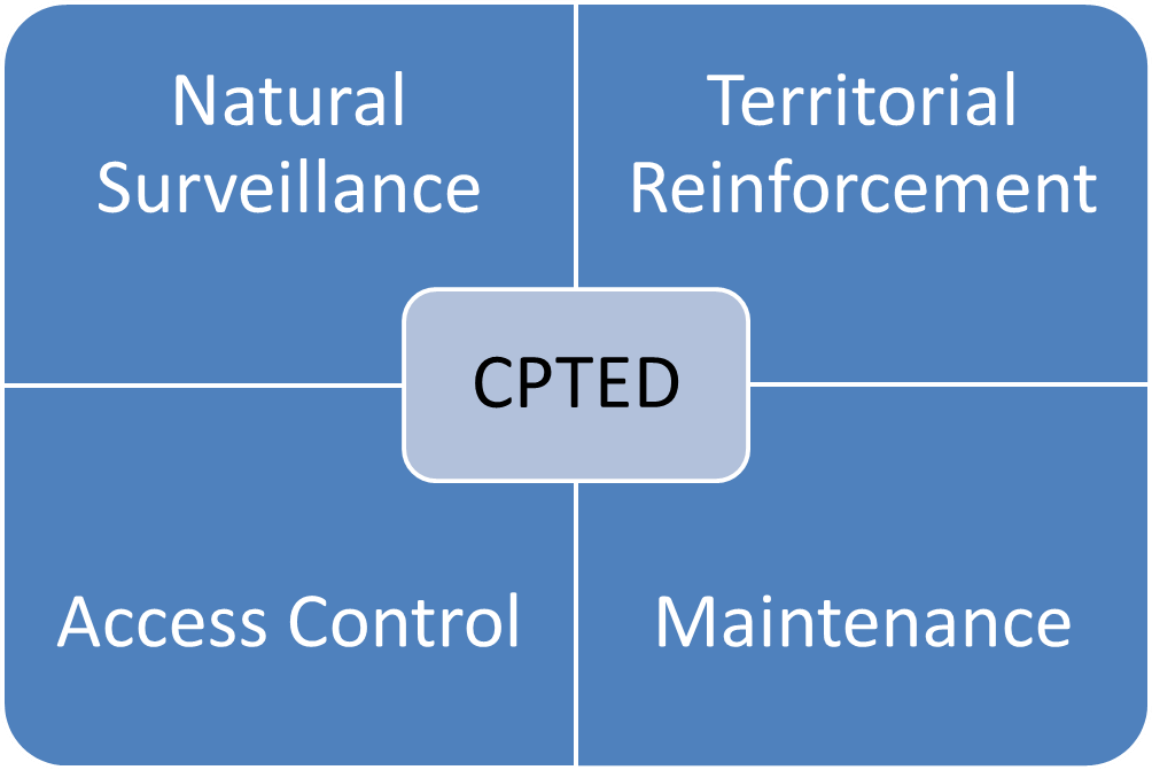
- Evolution of larger and more sophisticated drones
- Resiliency and Redundancy considerations
- Ongoing maintenance and refresh needs + spares
- Security Officer & LLE plans are part of the solution
- Physical Security Information Manager (PSIM) critical to success for large utilities

Look beyond facile/functional security to psychological and useful environmental solutions, especially during asset site refresh

Corporate Risk® SOLUTIONS

Beyond Physical Hardening:

Crime **P**revention **T**hrough **E**nvironmental **D**esign



Corporate Enterprise Security, Inc.

What is CPTED and Why Use it?

- Use of space (design) that deviates from more traditional target-hardening. Provides built-in Secure and Defensible Spaces to protect people, assets, and property
  - Industrial, Campus, Business – Multi-Use?
- Allows for more natural / normal uses of the environment without “fortressing”. Naturally Mitigates Designated Threats and Identified Risks.

  Graduated Scale of Control
  - Territorial Controls / Jurisdiction (signage, approaches, vehicle – personnel, lighting, clear areas (successive layers)
- Use of natural access control, natural surveillance view lines, and territorial reinforcement.

Process Recommendations

- Analyze and identify distribution critical infrastructure assets
  - Larger, connected substations
  - Substations that supply critical assets such as key businesses, LLE, medical facilities
  - Critical infrastructure services such as water supply and communications
- Utilize intelligence resources to develop a Threat Definition for Distribution
- Secure qualified resources to perform risk & vulnerability assessments of identified critical assets based upon the Threat Definition
- Develop security design for identified critical assets based upon the individual site security assessments to include maintenance and refresh requirements
- Develop a schedule for implementation/installation of the accepted site-specific security design(s)
- Performance based; *not* prescriptive

Corporate Risk® SOLUTIONS

Questions ?