Physical Security

Critical Infrastructure

RELIABILITYFIRST Security Working Group

February 14, 2021

Kevin T. Doss, MS, CPP, PSP

Level 4 Security

Kevin.Doss@Level4Security.com

- 30+ Years Physical Security Experience
- 15+ years Critical Infrastructure Protection
- ASIS PSP Board Certification Advisor/Instructor
- Southcentral PA Task Force
- Former Contract FERC Auditor
- MS Security & Risk Management – University of Leicester
- Certified Protection Professional (CPP) - ASIS
- Certified Physical Security Professional (PSP) - ASIS
- ASIS Physical Security Professional Study Guide Author
- Active Shooter Book Co-Author

Presentation Goals

1. Provide an overview on NERC CIP-014 Standards
   - Threat and Vulnerability Assessment Overview (R4)
   - Security Plan Overview (R5)
2. Discuss common physical security challenges for utilities
3. Physical security concepts
   - Performing Vulnerability Assessments (R4)
   - Security Plans (R5)
   - Security Measures (R4 & R5)

What level of protection do you need?

CIP 014-2 Standards R4

CIP-014-2 Requirements at a Glance

- R1: Risk Assessment
- R2: Unaffiliated third party risk assessment verification
- R3: Primary Control Center
- **R4: Potential threats and vulnerabilities evaluation**
- **R5: Physical security plan**
- R6: Unaffiliated third party R4 and R5 verification

CIP-014-2 Requirement R4

- The R4 evaluation must consider:
  - Unique characteristics of the identified and verified CIP-014-2 asset
  - Prior history of attacks on similar facilities
    - Frequency
    - Geographic proximity
    - Severity of past physical security related events
  - Intelligence or threat warnings
    - Law enforcement
    - Electric Reliability Organization (ERO)
    - Electricity Information Sharing and Analysis Center (E-ISAC)
    - U.S. federal agencies
    - Canadian government agencies

R4 Threat & Vulnerability Assessment

- Usually based on expert judgement using:
  - Asset Identification & Unique Characteristics
  - Threat Identification (history & intelligence, credible, likely, prioritized)
  - Security Effectiveness Assessment
    - Current protective measures
    - Threat Analysis
    - Vulnerability/Gap Analysis
    - Consequences (partial and total)
  - Recommendations
  - Security Design and Mitigation Elements (Planning)

R4 TVA Common Challenges

- Lack of expertise/knowledge
- Did not use established analysis tools (DBT, RAM, CARVER, etc.)
- No path analysis (Adversary Sequence Diagrams)
- Lack of layered protection schemes
- Obvious threats are not analyzed
- Overlook high impact/low frequency events
- Threat identification is generalized, not specific
- Improper ballistic threat and IED protection
- No planning for insider threats and collusion
- No rationale for including or excluding threats
- Recommendations are not completed or follow-up is lacking

CIP 014-2 Standards R5

CIP-014-2 Requirement R5

- The R5 security plan
  - Developed within 120 days of R2 verification
  - Executed according to specified timeline
  - Resiliency or security measures:
    - Deter, detect, delay, access, communicate, and respond
    - Vulnerabilities identified in R4 evaluation
  - Law enforcement contact or coordination information
  - Physical security enhancements and modifications timeline
  - Provisions to evaluate:
    - Evolving physical threats
    - Corresponding security measures

Physical Security Misconceptions

- All barriers offer similar protection.
- Detection (and assessment) may only utilize equipment/condition sensors.
- Detection (and assessment) should only be within the site perimeter.
- Assessment is often assumed if there are operable surveillance cameras present.
- The assumption of an effective response by an unarmed employee or security officer.

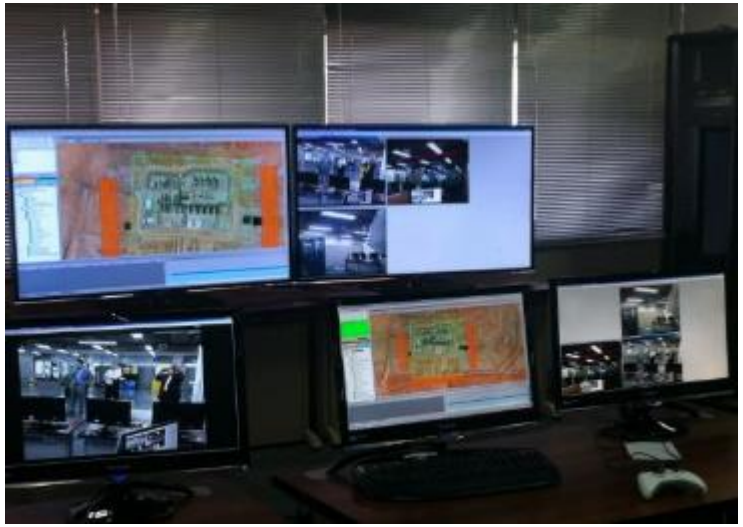
Photo used with permission.
Courtesy of AMICO Security.

R5 Security Plan Common Challenges

- Resiliency or Security?
  - Collectively must Deter, Detect, Delay, Assess, Communicate & Respond to the threats and gaps identified in the TVA (R4).
  - Single points of failure
- Evaluation of the effectiveness of chosen security measures by site
- Timeliness for deployment of countermeasures
- Law enforcement coordination, and lengthy response times
- Evaluation of evolving threats and countermeasures by site
- Assume that bad things can happen. Flexibility to adapt is critical.
- Using templates and boilerplates for different sites

Basic Concepts of Physical Security

1. Deter
2. Detect
3. Delay
4. Assess
5. Communicate
6. Respond



Feature Based Criteria

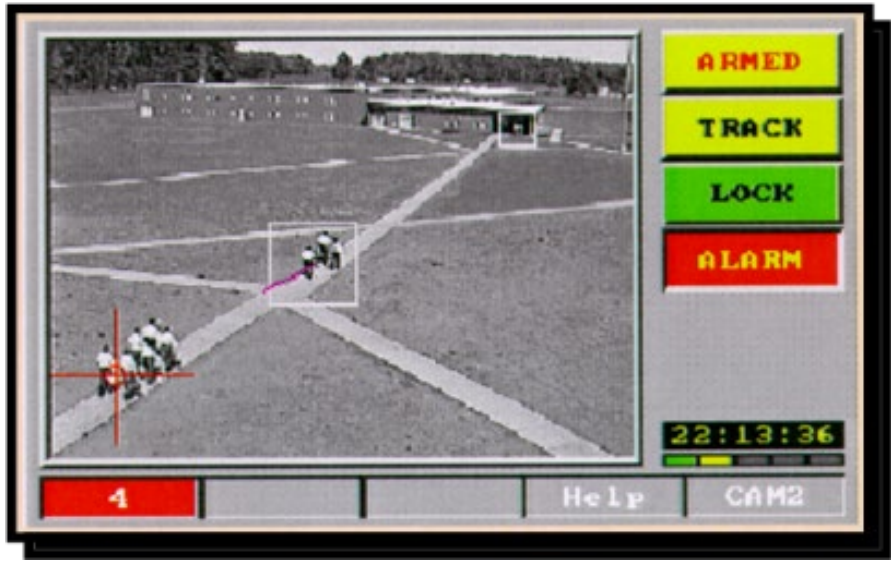
- Selects elements or procedures to satisfy requirements.
- Effectiveness measure is the presence of the features. (i.e. checklist only)
- Should generally be avoided or used with care
  - Will they perform as anticipated?
  - Will they work at night?
  - During inclement weather?
  - Under stress?
  - Are there any conflicts?

Performance Criteria

- Elements and procedures
  - Contribute to overall system performance
  - Not just a checklist
  - Baseline (existing) conditions verses requirements and amount of improvement can be determined.
  - Increase in system effectiveness verses the cost of program upgrades (Cost-Benefit)

Performance Testing of Systems

- Each device should be tested (Camera, intrusion sensor, card reader, lock, etc.)
- Each subsystem countermeasure should be tested (IDS, CCTV, Access Controls)
- The entire protection system should be tested for operation
- The entire system should be analyzed against all known and perceived (and potential) threats
- Document results



Perimeter Barriers

- Visibility
- Height
- Installation
- Reinforcement
- Ballistic ratings
- Intrusion sensors
- Vehicle ratings

Ballistic Threat Considerations

- Ballistic Protection should be based on identified threats
- Pistol and rifle calibers (Ratings)
- Approximate distances
- Consider vandals and accidental damages
- Site accessibility
- Response protocols
- Wind load / maintenance / engineering / oh yeah cost!

Image used with permission.
Courtesy of Ameristar/ASSA ABLOY

Image Source: Wikipedia

Gunshot Detection

- Coverage area
- Integration with video management
- Fixed/Mobile/Indoor/Outdoor
- Response force and protocols
- Privacy
- Budget

Protect Your Mobile Units

NERC CIP-014-2 Program Snags

- Focus on great security – do not just interpret the standards to meet the minimum level of protection.
- “It will never happen here”. Proven to be a wrong assumption.
- Accepting the risk. This is not appropriate for critical assets.
- Not meeting the timeline requirements and schedule for the program enhancement, risk analysis and implementation of security upgrades.
- Not involving engineering, operations and IT in the process.
- Using consultants that lack competency and knowledge.

You do not rise to the level of your goals.

You fall to the level of your program.

Final Thoughts

- Electricity = Life. I believe the greatest threat to our nation is an attack on the grid. The CIP-014 standards are designed to provide more than just physical protection; they have been developed to provide a holistic approach in preserving our nations critical infrastructure.
- Use a team approach. Everyone is important. If you don’t know something, find someone who does. Pride is the enemy of security.
- Lead. Do the right things. Develop, improve and inspire everyday.
- Adjust your sails. Solve problems.

Questions

Kevin T. Doss, MS, CPP, PSP

Level 4 Security

PO Box 665, Camp Hill, PA 17001

Email: Kevin.Doss@Level4Security.com

Website: www.level4security.com

Thank You for Participating!

Disclaimer: While every effort has been made to ensure the accuracy of the information presented herein and its relevance, the professionals who prepared this material do not make any representations or warrantees relative to its accuracy, usefulness or suitability for any particular purpose other than that of general study. It is not intended to be all-inclusive or an in-depth study of the subject material or regulatory requirements.