NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reducing Cyber Risk in the Bulk Power System: The Cyber Risk Preparedness Assessment (CRPA)

Michael Assante, Vice President & CSO, NERC

Tim Roxey, Manager Critical Infrastructure Protection, NERC

Mark Fabro, President and Chief Security Scientist, Lofty Perch, Inc.

SANS SCADA Security Summit March 24-28, 2010

Disclaimer

The material presented in this briefing is designed to provide guidance to registered entities in support of NERC Critical Infrastructure Protection compliance programs and to enhance registered entity understanding of cyber incident response functions that can support the reliability and availability of the North American bulk power system.

This material is provided as-is and is not intended to replace or make obsolete any current cyber security activities of an entity. NERC takes no responsibility for how the material presented in this briefing or resulting outputs are used. This material may not be used for commercial purposes of sale to or use with other third parties without prior written consent from the North American Electric Reliability Corporation.

Agenda

- Background
- Meeting the Challenges
  - Objectives and Goals
- Exercise Approach
- Findings and Conclusions
- The Path Forward
- Q&A

Background

- The Cyber Risk Preparedness Assessment (CRPA) was developed to answer the need for more granular understanding of BPS entities cyber risk profile.
- The project designed to assess the current cyber resiliency capabilities of BPS entities and the adequacy of existing reliability mechanisms related to the highly unique nature of cyber threats.
- By conducting such an assessment, NERC can target key areas for improvement and areas of best practices (successes) can be shared with industry
  - In addition, government information sharing activities and Electricity Sector Information and Analysis Center ("ES-ISAC") operations can be assessed as well.
- By working with stakeholders, the CRPA will serve as a benchmark that can be used to identify focus areas

Meeting the Challenge

- Identify and prioritize significant technical concerns such as attacker tactics against critical infrastructure systems, telecommunication paths and general/special information technology networks
- Identify specific needs for improved research and development into advanced intrusion prevention, intrusion detection, holistic system defense, unique technology vulnerabilities, cyber security testing, and security tool development
- Identify mitigation and recovery strategies, and
- Assess levels of training needed for personnel working in the area of cyber security and BPS reliability.

Important

- It is important to note that the CRPA is not a test, nor is it an activity to inspect, evaluate, or audit compliance with NERC CIP Reliability Standards.
- CRPA is not a mandatory program. The goal of the program is to obtain a detailed understanding of capability gaps and associated mitigation measures, and to provide for effective resilience and recovery activities as it pertains to the cyber security of the BPS.
- The participation of volunteer entities with responsibility for the reliability of the BPS is ***critical to success***.

Objectives – General

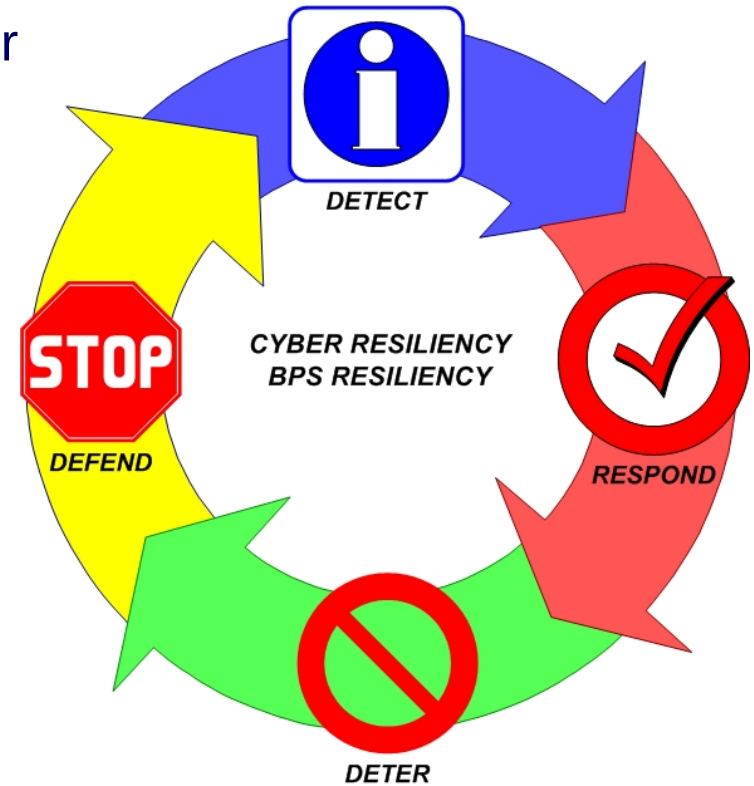
- Enhance resilience and reliability of the entity
- Enhance both proactive and reactive capabilities that are
  - Specific to an entity
  - Beneficial to the entire NERC community of entities
- Learn detailed prescriptive knowledge based on ground-truth scenarios
- Understand the realistic ‘gaps’ in cyber preparedness

Objectives - Granular

- **Discuss Pre-incident Threat/Vulnerability Assessment and Risk Mitigation**
  - Risk assessment process
  - Internal Business Unit (BU), Cross-BU and External Communications:
  - Collaborative risk mitigation implementation
  - Resource implications and impacts
- **Examine Interdependencies for Cyber Incident Response**
  - Incident identification and escalation process
  - Cross-BU collaboration, reporting and incident assessment (including escalation procedures)
  - Whole of business coordination (C-suite, Public Affairs, IT, Operations, Field Svcs)
- **Explore Collaborative Aspects of Post-Incident Actions and Recovery**
  - De-escalation
  - Cross-BU prioritization and resource allocation
  - Reporting
  - Post incident assessment
    - Security posture / controls
    - Response process

Goals

- Understand impact of cyber attack on the entity
- Observe and improve current procedures and practices utilized by the entity to deter defend, detect, respond to, and recover from cyber attacks
- Catalog how the entity implements best practices for responding to cyber related incidents impacting the BPS
  - Incident Response Plans
- Explore strategies to improve cyber risk management and the cyber security posture of the entity



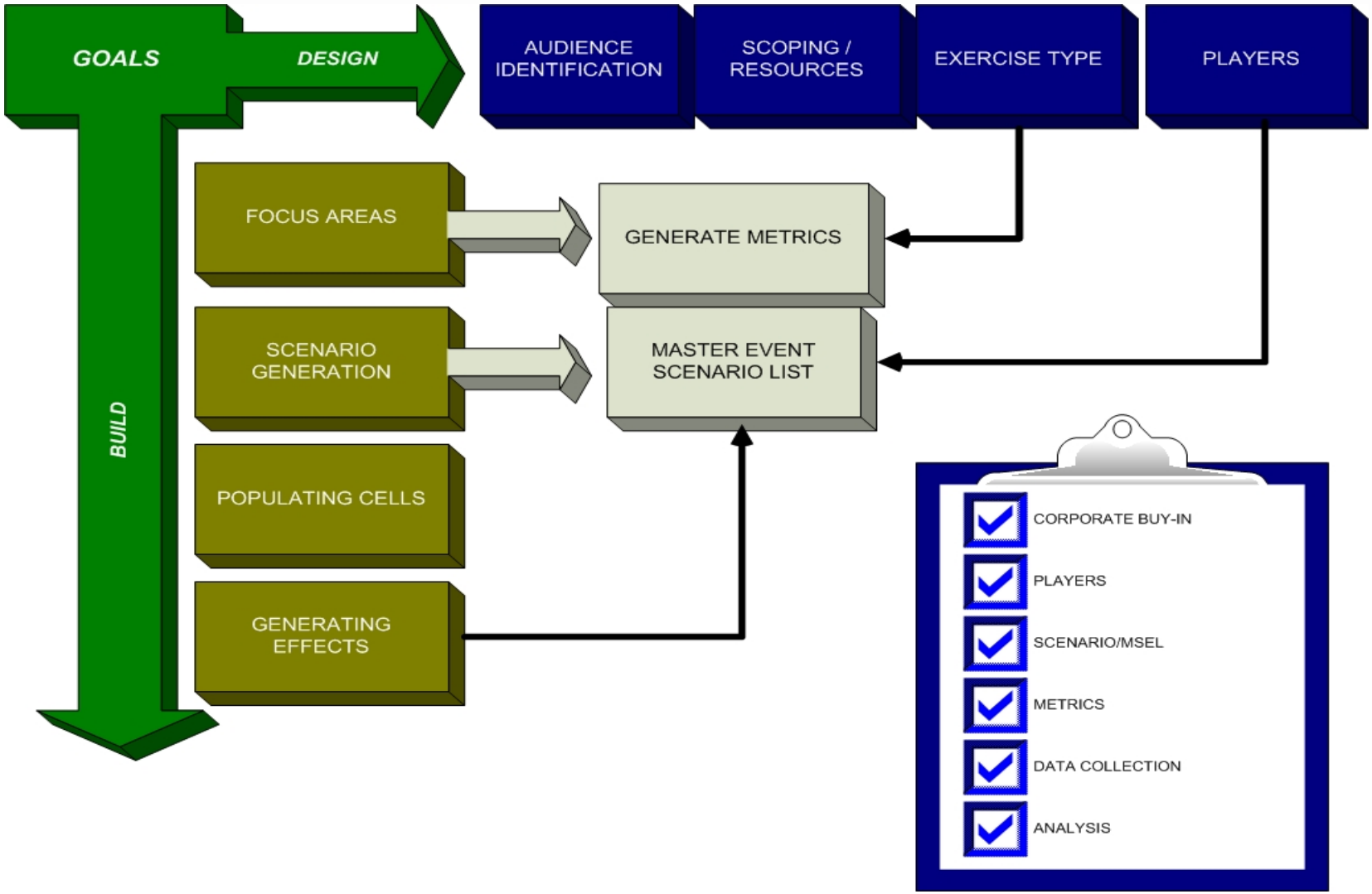
Goals

- Train staff so that operational efficiency is improved during actual incidents
- An incident response exercise can target different or multiple audiences
  - Incident response can include a multitude of departments, or just one, depending on the type of incident and how easy it is to solve
  - Exercises should be planned so that every staff member who would be involved in an actual incident receives some form of training each year.

Ensuring Applicability

- Leverage technically grounded cyber threat scenarios
  - Determine how BPS entities might detect, respond, mitigate and report cyber incidents
  - Identify any capability gaps in their cyber security posture. This in turn will be used to identify steps required to improve overall BPS preparedness.
- The scenarios are used to assess entities' preparedness based on the following capabilities to:
  - Detect cyber attacks (using lessons learned from known actual cyber events);
  - Prevent cyber attacks;
  - Technically respond to cyber attacks;
  - Manage their electronic systems and electric assets to minimize potential damage;
  - Communicate and coordinate effectively with interconnected neighbors and Reliability Coordinators to contain the effect on the BPS; and
  - Communicate and coordinate effectively with appropriate local and federal authorities

General Exercise Framework



TTX Overview

- The exercise usually consist of at least three “moves” that will progress the participants through the incident response cycle:
  - Move 1: Pre-incident Threat/Vulnerability Assessment and Risk Mitigation
  - Move 2: Incident Response
  - Move 3: Incident Closeout and Recovery
- Participants are enrolled to work through their response to the exercise scenario(s) as part of various ‘Breakout Groups’. For example:
  - Management: Emergency Management, Incident Response, Physical Security, Senior Management
  - IT - Corporate
  - EMS - SCADA
  - Control Center Operations
- Additional Breakout Groups may be formed based on established procedures
- Field Services and External entities (ES-ISAC, NERC, etc.) are represented by “white cell” players

Realism: Exercises vs. WarGames

- A strong factor in determining both player engagement and usefulness of observations
  - TTX will employ actual incident response plan
- Should align with scope and targets of evaluation
- Absence of 'silliness' can be beneficial
  - No global malware attack (assume the Internet works fairly well)
  - No continent-wide earthquakes of magnitude 9.0
  - No alien invasion (or threat of alien invasion)
  - No extinction-level solar flares or meteors
- Easier to create scenario, but more importantly easier to create branches, sequels, and just-in-time injects

Branches and Sequels

- There is a definitive requirement for providing flexibility into the exercise to preserve freedom of action under rapidly changing conditions.
  - Players do not accept scenario (very common)
  - Players have to leave (more common that we would like)
  - Incidents impact game play (fire drills, illness, tech failures)
  - Players need additional stimulation (rare but nice to see)
- Branches
  - Contingency plans or options built into the basic TTX (usually hidden from play) for changing the disposition, orientation, or direction of movement, and for accepting or declining scenario components of the MSEL. Provides Master Facilitator flexibility by anticipating player reactions that could alter the planned exercise structure.
- Sequels
  - Subsequent activities that are based on the possible outcomes of the current and planned exercise activities Sequels feed Master Facilitator is a continuous process during an operation so that the commander always has options.

CRPA MSEL Elements

- The technical scenario is factual and based on open source and derived intelligence from actual architectures
  - Real network and device names
  - Real protocols and vulnerabilities
  - Real incident response plans

Justification for CEII classification

- Elements of historical exercise types are included
  - For comfort and for realism
- TTX uses actual alerting formats and non-fictional events
- TTX uses proven gaps observed in field assessments
- TTX scope is very well defined
- Branches and sequels are anticipated and build prior to every TTX

Caution: Artificialities and 'Steering'

- Need to be aware of these to tune observations and findings
- There are several root causes for these:
  - Pace impacts communications
  - Scenario is often expected to be only cyber (when it is generally not)
  - Availability of players impacts feasibility/success of certain scenario elements
  - Tempo can create chaos
- Steering needs to be avoided
  - TTX should naturally produce measurable findings and gaps
  - Must be attentive to the urge to guide towards desired behavior

Findings

- **Strong Leadership**
  - Management teams quickly establish their leadership in managing the incident, rapidly coordinating communications between groups and to outside stakeholders, and establishing a decision-making framework for the incident.
- **Excellent Communication**
  - all 'player' groups establish clear lines of communication with each other as the incident began and progressed.
- **Use of Incident Response Planning**
  - Strong presence of working or DRAFT incident response plans, many of which are comprehensive and clearly impact response activities
- **Self-Organizing**
  - Entities are very capable at self-organizing under duress
- **Operational Priorities**
  - Operational priorities are obvious, with activities and choices driven to the protection and availability of the electrical grid.

Findings (cont.)

- Skepticism regarding possibility of cyber attack
  - Foundations for this are often cultural
  - Difference between ‘possibility’ and ‘possibility of attack success’
- Incident response activities are not fully understood by all key employees
  - Although plans can be well understood, how to put activities ‘into-action’ can sometimes be poorly understood
  - Improvements can be made by adding SCADA/ICS support into IR/Forensics reams
- Some need for clarity as it relates to when and how to contact law enforcement
  - Seemingly trivial activities are actually very hard (as are expectations regarding LE response processes)
- Entities generally unsure of how to interact with RC during a cyber incident
- Challenges for those entities having one core discipline are very different for those that have multiple (TO vs TO/LSE/DE)

Findings (cont.)

- The ability to respond to physical incidents is exceptional, and aligns with current level of expectations for those responsible for BPS reliability
- Assessment and integration of alerting materials and advisories from ES-ISAC and/or ICS-CERT shows reporting is very useful
  - Entities have a clear understanding of ISAC roles and communications protocol
  - TTX can highlight deficiencies as to who in the entity is not getting pertinent need-to-know information

Findings (cont.)

- Specific critical path items
  1. Modification of restorative / fail-over procedures to ensure limitations of cyber impact
  2. Refinement of physical incident response plans to incorporate for consideration of impact to cyber-risk profile
  3. Increase granularity of security training so it is prescriptive to cyber incident response (test what you do NOT know)
  4. Extend the audience for IR training, specifically augmenting teams to include SCADA/ICS members
  5. Standardized process/protocol for involving law enforcement
  6. Standardized process/protocol for interacting with peers and coordinators during cyber crisis

Current NERC Activities

- Help support the refinement of the collaborative process between entities, ES-ISAC, law enforcement and other key stakeholders
  - Getting the right information to the right people at the right time
- Categorization of cyber incident types and their impact to the BPS
- Develop technical guidance regarding the mitigation of critical findings
  - Exploit success of entity countermeasures and extend to the larger community
- Create the applicable prescriptive knowledge needs for BPS entities to mobilize best practices for incident response
- Formulate the research plans to address ground-truth findings that may be ubiquitous across BPS entity types
- Create the framework for the Gap Analysis function so that it can change organically with more stakeholder interaction

Future Planning

- Longer exercises to facilitate a real-time set of activities
- Greater integration with ES-ISAC and LE response measures
- Multi-national/multi-entity scenarios
- Refinement of exercise kits for NERC entities for CIP compliance efforts
- Greater enrollment efforts via NERC CIPC channels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Thank You

Questions?

For more information in CRPA, please contact:

Tim Roxey, Manager Critical Infrastructure Protection

tim.roxey@nerc.net