Status of Cyber Security for U.S. Nuclear Power Reactors

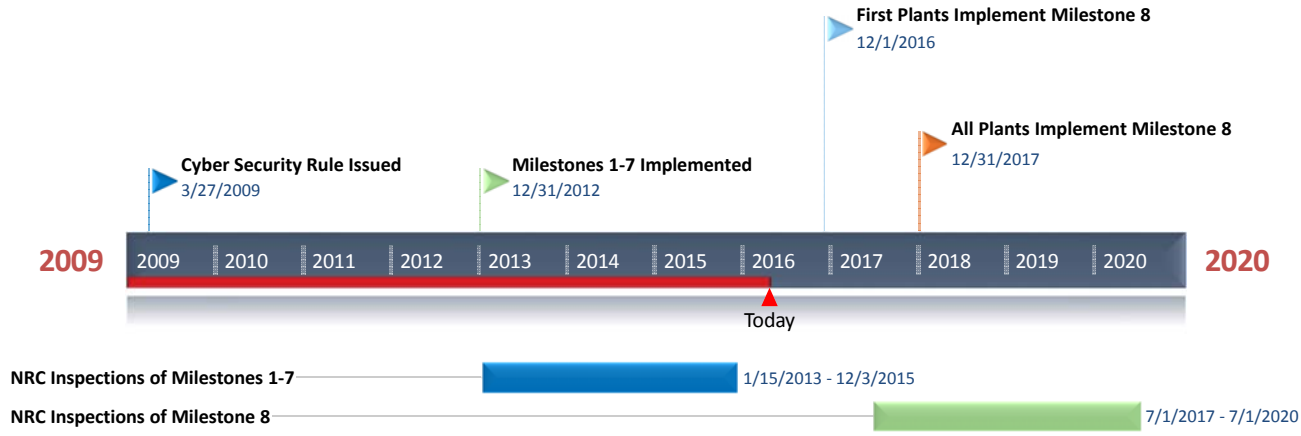
William Gross
Senior Project Manager, Security
Korean Nuclear Society Meeting
May 11, 2016 • Jeju Island, Korea

Presentation Topics

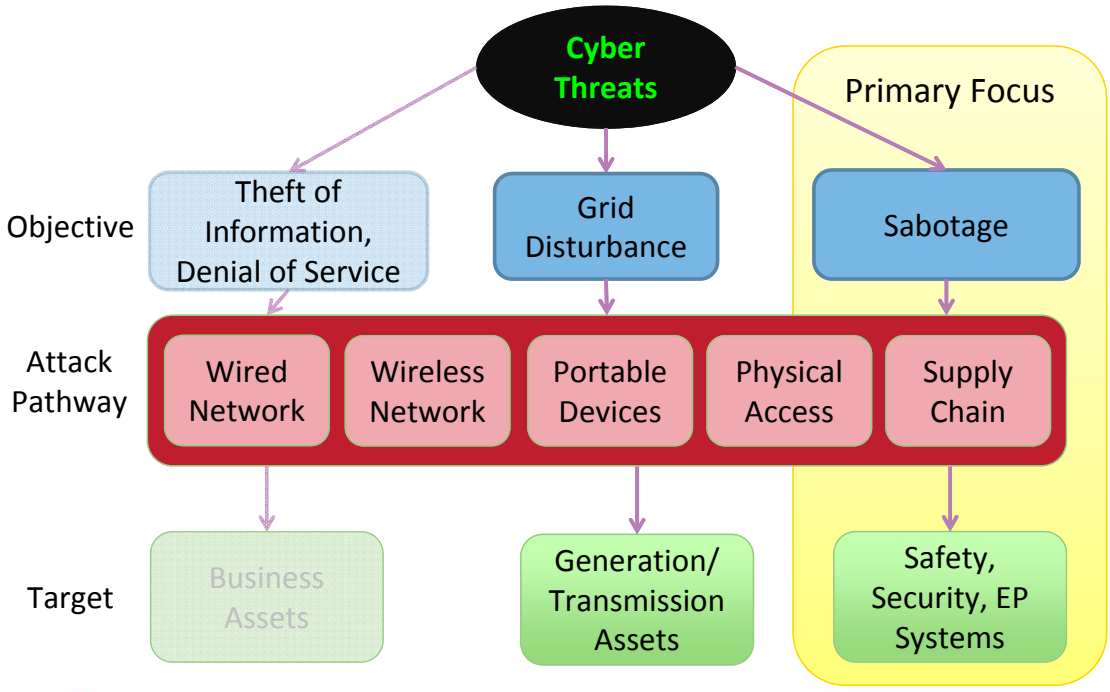
- The cyber plan implementation milestones
- NEI 10-04 and NEI 13-10 guidance documents
- Technical security control implementation
- Roles and activities of NEI, NITSL, EPRI, INPO

NEI NUCLEAR ENERGY INSTITUTE nuclear. clean air energy.

Cyber Plan Implementation



Milestone 1-7 Protection Concept



Milestone 1-7 Measures Implemented

- Form a cyber security team
- Identify digital assets requiring protection
- Isolate the plant from all network access
- Implement comprehensive controls over portable media and mobile devices
- Enhance insider mitigate programs
- Implement and maintain cyber controls for essential assets

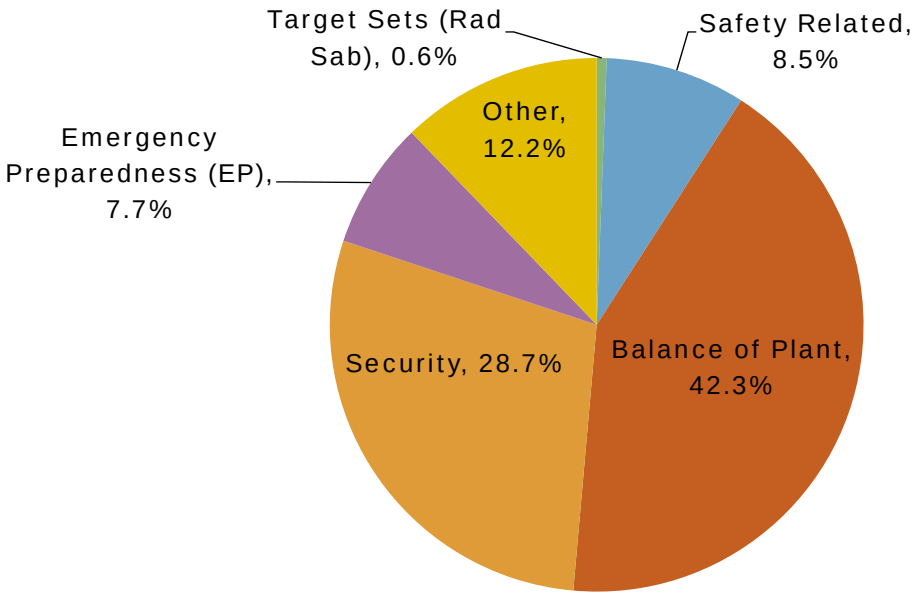
NEI 10-04 – Identification of Digital Assets

- NEI 10-04 provides guidance for identifying digital assets requiring protection
- While the principal concern is on reactor safety, NEI 10-04 includes balance-of-plant
  - Balance-of-plant included to address digital assets that would otherwise be subject to Federal Energy Regulatory Commission cyber requirements
- NEI 10-04 has not changed in several years

NEI 13-10 – Addressing Security Controls

- The Cyber Security Plan (from NEI 08-09) was designed for small numbers of digital assets
- Licensees identified thousands of digital assets
- NEI 13-10 developed to grade implementation using a consequence based approach

Driver for a Consequence Based Approach



Est. >1,000 CDAs per plant unit

A System Assessment

Consequence Approach Implementation

- Provision assets based on impact of attack
- Indirect assets
  - No direct impact to safety, security function, or
  - Consequences mitigated prior to impact.
  - Includes low impact EP and balance of plant assets
- Direct assets - those not identified as indirect
- Cyber security controls graded

Benefits and Future Applications

- NEI 13-10 approach working well for reactors:
  - Achieving desired outcomes (75% or more indirect)
  - Permits licensees to focus on high consequence assets
- Improvements if considered for other licensees:
  - Not all functions are equally attractive to an adversary seeking to harm the health and safety of the public
  - Prioritize only those assets that if compromised would likely result in radiological sabotage or theft of SNM
- Best - eliminate any system not directly related to preventing radiological sabotage

Technical Security Control Implementation

- NEI 13-10 provides control implementation guidance
  - Section 5 provides a reduced set of security controls for Indirect assets
  - Section 6 and Appendix D provides pre-developed assessments for Direct assets that have limited functionality
    - Pre-developed assessments can be applied to classes of devices that have similar technical capabilities

Technical Security Control Implementation

- Implemented controls protecting digital assets
  - Isolation, wireless not used or greatly restricted
  - Portable device controls
- Device-specific controls being evaluated
  - User accounts, permissions, and password
  - Logging and analysis capabilities (SIEM)
    - Generally for high-functioning assets (plant computer)
  - Disabling or preventing access to unused ports

Technical Security Control Implementation

- I do not see:
  - Device or network encryption
    - Except in the physical security systems
  - Modifications to existing assets to add new functionality to support cyber controls
  - Directly connecting isolated assets or networks to support log data collection
  - Passwords on HMIs in the main control room

NEI

- NEI - Nuclear Energy Institute
- Provides principal coordination between the utilities and the NRC
- For cyber security, focus is on acceptable methods to comply with NRC requirements
- The NEI Cyber Security Task Force reports to NEI Security Working Group, which reports to Nuclear Strategic Issues Advisory Committee

NEI Engagement with NRC

- NEI engages NRC through public and closed meetings to discuss issues including cyber
- NEI provides comments to NRC during guidance development
- NEI may develop guidance and provide to NRC for endorsement. Issues identified by NRC's reviews are corrected in final document.

NITSL

- NITSL – Nuclear Information Technology Strategic Leadership
- Has a Cyber Security Standing Committee
- Technical support to plants on program implementation
- Directly supports the NEI Cyber Security Task Force

EPRI

- EPRI – Electric Power Research Institute
- Provides technical research
- Established a cyber security technical advisory committee
- Many cyber products developed or under development that are beneficial for nuclear plants

INPO

- INPO – Institute for Nuclear Power Operations
- Integration of cyber elements into digital design reviewed during evaluations
- Developed cyber security training modules

Resources

- NEI 08-09, Revision 6 – (ML101180437)
  - Provides template for Cyber Plan
- Implementation Schedule – (ML110600218)
  - Template for the implementation schedule
- NEI 10-04, Revision 2 – (ML12180A081)
  - Describes identification of digital assets for protection
- NEI 13-10, Revision 4 – (ML15338A276)
  - Consequence-based approach to cyber controls
  - Pre-developed assessments for low-function digital assets

QUESTIONS

William Gross
wrg@nei.org
(202) 739-8123