Perspectives on Risk Informing Cyber Program Implementation

William Gross
Senior Project Manager, Engineering
INMM Reducing the Risk Workshop
March 18, 2015 • The George Washington University

History of Addressing the Cyber Threat

2002-2004

- NEI Cyber Security Task Force Formed
- Interim Compensatory Measures (ICM) Order
- Work Hours, Training and Revised DBT Orders
- NRC Completes Cyber Assessment Pilot Program
- NUREG\CR-6847, "Cyber Security Self-Assessment Method"

2005-2007

- NEI 04-04, "Cyber Security Program for Power Reactors"
- NRC Endorses NEI 04-04
- NEI, NERC MOA, NEI 04-04 Equivalent to CIPS 002-009
- NSIAC Voluntary Initiative for Cyber Security Programs
- RG 5.69, "Design-Basis Threat"
- Cyber Attack Added to Design Basis Threat

2008-2010

- NEI 04-04 Implemented
- NRC Cyber Rule Issued
- NRC Endorses NEI 08-09, Cyber Plan Template
- FERC Order 706-B Resolution

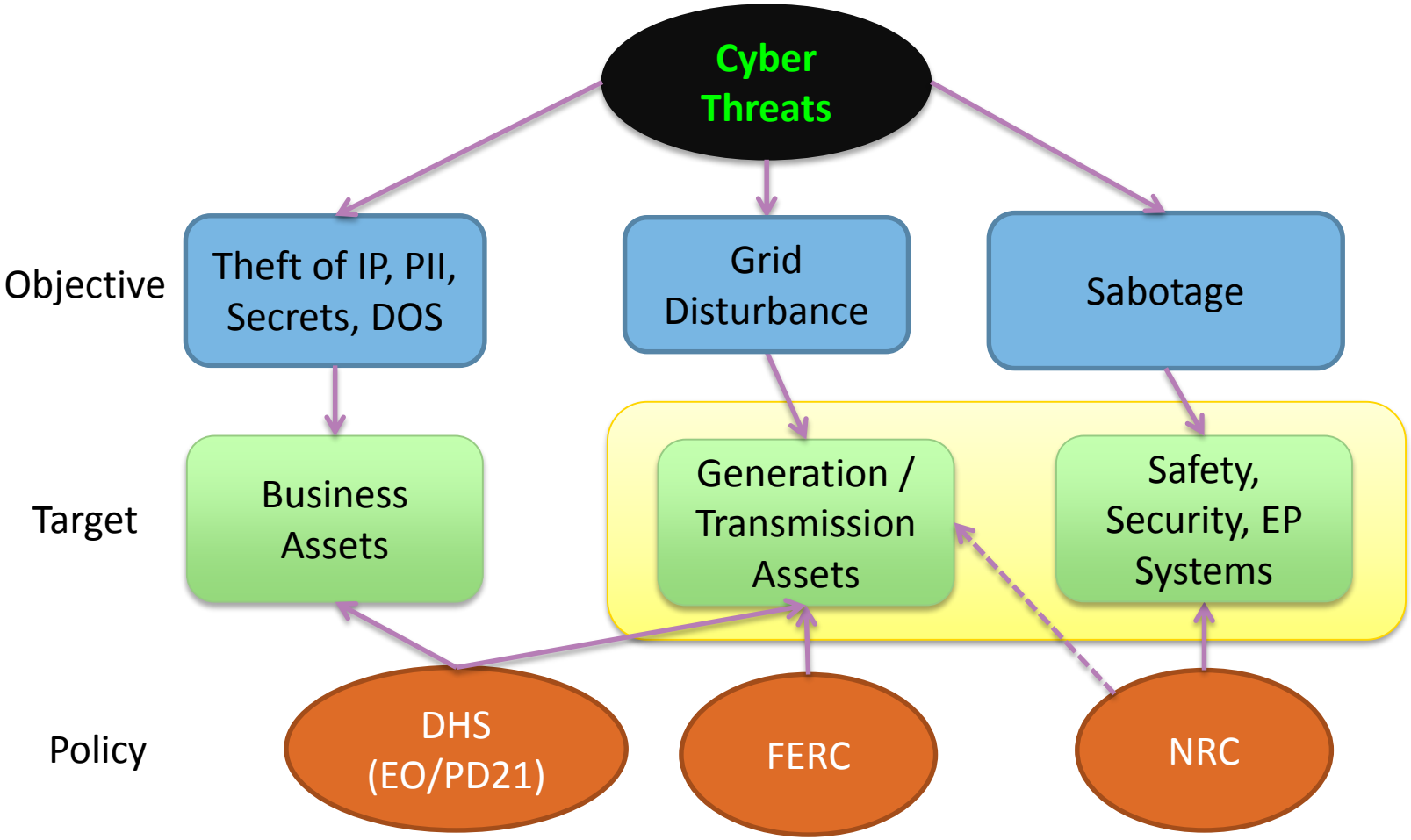
2011-2013

- NRC Endorses Cyber Plan Implementation Schedule Template
- NRC Approves Plans
- Milestones 1-7 Implemented
- NRC Inspections Begin
- Presidential Executive Order and Policy Directive 21

2014-2017

- Full Program Implementation

Threat Objective, Target, and Public Policy

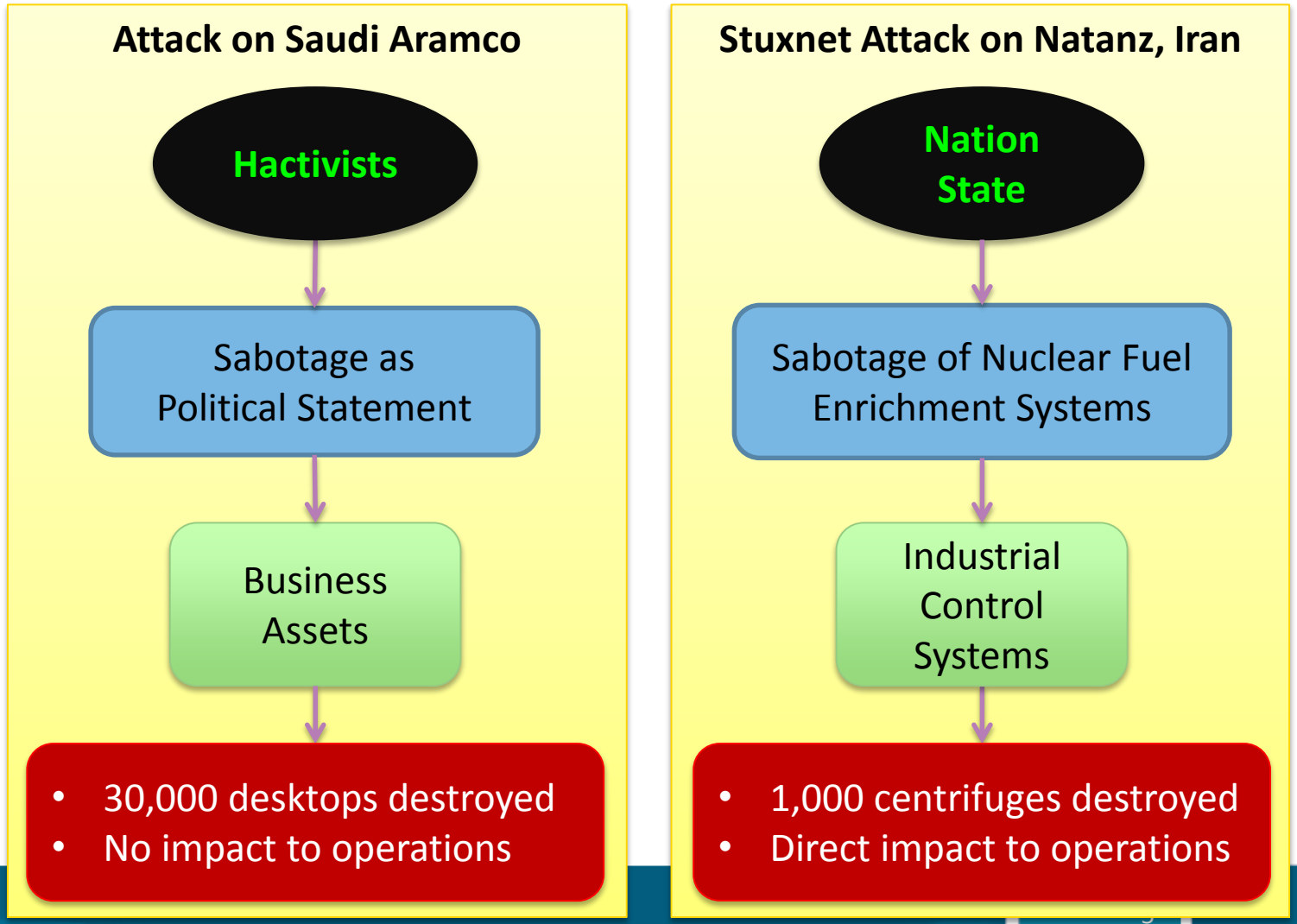


Cyber Security – The Concern for Nuclear

- A cyber attack is a tool an adversary may use in an attempt to directly or indirectly harm the health and safety of the public by exposure to radiation.

- Cyber security programs are designed to minimize that potential.

Example: Saudi Aramco VS Stuxnet



Elements of Effective Policy

- Performance objective clearly stated
  - "The program must be designed to prevent…"
- Implementation is risk informed
  - Effort commensurate with risk reduction achieved
- Requirements are performance based
  - Prevents static, compliance-based implementation
- Simple and easily understood

Risk-Informing Cyber Security Programs

- Risk insights can be used to inform
  a) The scope of assets identified for protection
     - E.g., protect SSCs associated with safe-shutdown
  b) The level of effort applied toward protection
     - E.g., controls increase based on asset risk significance
  c) A combination
- U.S. implementation uses option “C”
  - Broad set of assets covered, with graded controls

Areas for Consideration

- Simplicity cannot be overstated
  - Is there significant value from increased analysis?
  - Don’t we already know what is risk-significant?
  - Plant personnel are not, and need not be cyber experts.
  - Where standards are available, they should be considered.

Discussion

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