U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Risk-Informed Security: Summary of Three Workshops

N. Siu

Office of Nuclear Regulatory Research

U.S. Nuclear Regulatory Commission

Presented at

INMM/ANS Workshop on Safety-Security Risk-Informed Decision-Making

Sun Valley, ID, USA; April 26, 2015

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Workshops

- Risk-Informed Security Regulation
  - Albuquerque, NM
  - September 14-15, 2010
- Risk-Informed Security
  - Stone Mountain, GA
  - February 11-12, 2014
- Reducing the Risk
  - Washington, DC
  - March 17-18, 2015

Workshop on Risk-Informed Security Regulation (RISR) – Overview

- Location (Dates): Sandia National Laboratories (September 14-16, 2010)
- Sponsor: USNRC/RES
- Objective: Identify opportunities for improving risk-informed security regulation
- Discussion groups
  - PRA
  - Large facilities and transportation
  - Small facilities and transportation
  - Design Basis Threat vs. Graded Security Protection
- Participants: 52 (National Labs, Government Agencies, Universities)
- Workshop summary report sensitivity level: OUO

Workshop on RISR – Conclusions*

Six areas of opportunity and associated recommendations

- Examine the initiating event and its uncertainties
- Utilize simulation tools to supplement current approaches
- Promote collaboration
- Take a long-term approach to cyber security
- Establish security metrics for regulation
- Consider a security risk analysis effort equivalent to WASH-1400

*See P. Pohl et al., "Risk Informed Security Regulation (RISR) Workshop," presented to the INMM Risk Informing Security Workshop, Stone Mountain, GA, February 11, 2014.

Workshop on RISR – Additional Observations

- Participants generally accepting of risk-informed concept, recognized commonalities
- Challenges
  - Initiating event likelihood
  - Dependencies
  - Information sharing
- Alternate approaches to risk management
  - Conditional risk
  - Difficulty/consequence-based
  - Simpler methods for small facilities
- Need to recognize different regulatory applications
- Field is dynamic – ongoing developments may be helpful

INMM Workshop on Risk-Informed Security – Overview

- Location (Dates): Stone Mountain, GA (February 11-12, 2014)
- Keynote presentation: Commissioner G. Apostolakis (USNRC)
- Technical Sessions
  - Safety/security risk approaches
  - Material categorization
  - Initiating events/attack frequency
  - Vulnerability assessment simulation tools
  - Cyber security
  - Security risk management methods
- Participants: ~75 registered (National Labs, Government Agencies, Industry, Universities, International)
- Presentations

http://www.inmm.org/Risk_Informed_Security_Workshop1.htm

INMM Workshop on Risk-Informed Security – Conclusions*

- Risk assessment is a useful tool to support security-related decision making
- Frameworks, methods, models, and tools exist and are being used
- There remain considerable uncertainties in key parameters (e.g., likelihood of attack)
- Useful to benchmark available simulation models to better understand how and where their results differ
- Need to avoid stovepiped analyses
- Need to better communicate results and insights of security-related risk assessments
- Alternative risk management approaches (e.g., “fix vulnerabilities as they’re identified,” prioritize based on “attack difficulty” and consequences rather than risk) may be useful in practical applications.

*See J. Rivers, et al., “Risk Informed Security Workshop,” Institute of Nuclear Materials Management (INMM) Annual Meeting, Atlanta, GA, July 20-24, 2014.

INMM Workshop on Risk-Informed Security – Additional Observations

- Keynote speech
  - Risk-informed security should be a goal
  - Need to identify/focus on important scenarios, avoid excessive conservatism
  - There are many challenges and limited resources; need to start thinking
- Practitioners not necessarily enthused about assessing absolute likelihoods of initiating events but many (not all) still do it
- Virtues of systematic, integrated analysis with explicit consideration uncertainties well appreciated
  - Integrate expertise from multiple disciplines
  - Explicit assumptions
  - Identify and explore large number of possibilities
  - Generate potential surprises
  - Facilitate benchmarking and validation

INMM Workshop on Reducing the Risk – Overview

- Location (Dates): Elliot School of International Affairs, George Washington University (March 17-18, 2015)
- Keynote presentation: Dr. D. Huizenga (USDOE)
- Technical Sessions
  - Perception of nuclear risk
  - Global nuclear summit: the changing relations with Russia
  - Reappraising nuclear security strategy
  - Insider mitigation
  - Cyber security
- Participants: ~45 (National Labs, Government Agencies, Industry, Universities, Public Interest, International)
- Presentations: will be available from www.inmm.org
- House rules: no attribution outside of workshop

INMM Workshop on Reducing the Risk – Observations

- International interest in risk-informing safeguards as well as safety and security
- General agreement: need to use risk to focus on right things
- Sample viewpoints
  - Probabilities can be used when data are available; otherwise put heavier weight on consequences.
  - Explicit recognition of uncertainties and analysis transparency are critical.
  - Scenario likelihood can be difficult to communicate.
  - Important to communicate qualitatively, but easy to poke holes; need quantitative analysis.

INMM Workshop on Reducing the Risk – Observations (cont.)

- Sample viewpoints (cont.)
  - Terrorism is just another initiator.
  - Regarding human behavior and insider threat, “too many equations to solve.” Focus on prevention.
  - There is a significant amount of technical and behavioral data on (non-nuclear) insider threat, lots of observables.
  - Need to be careful using incident data; potential problem with false positives.
  - Risk = f(threat, vulnerability, consequence).
  - Graded approach needed in cyber; need to figure out what critical digital assets matter.
  - Need to distinguish between easy and difficult attacks.
  - Threats are changing.
  - Area is spending insufficient effort on biggest cyber risks.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

A similar trajectory?

"Debate within NRR appears to have moved beyond whether risk insights should be integrated into NRR activities, to discussion of how and when to implement risk-informed approaches."

- Wight, et al., 2002

E. Wight, L. Peterson, M. Caruso, A. Spector, S. Magruder, R. Youngblood, and K. Green, "Report on Interviews and Focus Group Discussions on Risk-Informed Activities in the NRC Reactor Program," Prepared for Nuclear Regulatory Commission Under Contract No. NRC-03-00-003," 2002. (ADAMS ML022460161)