Threats, Defined:

Updates from INL

11 Feb 2013

Bri Rolston

www.inl.gov

Idaho National Laboratory

Obstacles to Managing Cyber Risk

- Cyber risk in general
  - Defined only in terms of technology or technical capabilities
    - TTL for 0-day and detection
    - Number extant vulnerabilities on a system
    - Known exploit techniques
  - Viewed as a punishment or an obstacle to getting work done
  - Driven by compliance
  - Not clearly understood by most stakeholders
- Cyber risk in CIP environments
  - See above
  - Multiply those factors by a lot

Adding to the Chaos of CIP Cyber Risk

- Technology isn't used the same way anymore
  - Isn't used to improve efficiency
  - All about how data is aggregated and consumed
  - Consumerization of technology (BYOD, anything as-a-Service)
- Development of hybrid relationships
  - Government and industry
  - National security groups and industry
  - COTS and ICS/OT
- Conflicting risk management goals
  - Operations vs IT
  - Business vs national security
- Technical security architecture doesn't match threatscape
  - Candy bar theory of security architecture
  - Adversarial-based focus

Cyber Risk Management Goals

- General cyber risk goals
  - Provide a clear and consistent mechanism for evaluating cyber risk
  - Ensure cyber risk is considered equivalently to other enterprise risk
  - Define how technical data is mapped to risk management variables
  - Include technical characterization process for cyber components
  - Not be expressed in terms of technical security
  - Drive business process improvement
  - Encourage facilitation and collaboration across enterprise
- CIP goals
  - Demonstrate how cyber risk management improves resilience
  - Integrate with existing RCFA, BI, and ERM processes
  - Take advantage of cross-mapping controls to mitigate risk

INL's Cyber Risk Research

- DOE-OE funded 2 projects related to cyber risk in CIP
  - Root Cause Security Analysis Model (RC-SAM)
  - Advanced Cyber Threat Characterization (ACTC)
- Research focus
  - RC-SAM
    - Mapping technical security data to risk variables
    - RCFA analysis process for cyber incidents
  - ACTC
    - Consistent technical threat characterization
    - Linking threat data to risk management

Consideration 1: Impact to OT/ICS

- IF Cyber Risk to OT & CIP networks =
  - Probability x Impact
- WHERE CIP impact
    - Is typically a physical result that impedes the ability to complete an automated process as required
  - AND
    - Is realized during any event in which cyber resources affect organizational ability to complete an automated process as required
- THEN cyber security efforts
  - Are relatively restricted in terms of how they can minimize risk
  - Can't generally do much to minimize physical impact
  - Mostly focused on decreasing probability
- END IF

Consideration 2: Differing Risk Equations

- Two primary equations
  - Risk = Probability x Impact
  - Risk = Threat x Vulnerability x Consequence
- Risk equations are important to data mapping
  - Necessary to compare cyber risk equivalently
  - Organizes cyber data in a way everyone can understand
  - Makes sure have a more holistic understanding of risk
- Context matters
  - Different uses for each equation
  - Technical cyber security data should be mapped to one of the variables
  - Variable mash up confuses everyone

Consideration 3: Differing Risk Goals

- Big difference in the way risk is considered by:
  - Corporate world
  - National security groups (feds, law enforcement, military, DHS, intel community)
- Corporations use R = P x I
  - Don't care WHO causes the problem
  - Care about impact to service and the bottom line
  - Not critical in the incident response process to address threat
- National security groups use R = T x V x C
  - Do care about who poses a threat
  - Have the resources necessary to gather and generate effective threat intelligence assessments
  - Critical for these groups to characterize threat so can plan response

RC-SAM : Data Organization & Analysis

- RC-SAM → all about mapping technical data to risk variables
  - Dependent on cyber security order of operations
    - People
    - Process
    - Technology
    - Security
  - Uses Functional Security Matrix (FSM) for relationship mapping
  - Based on common RCFA techniques
- Results in
  - Methodical approach to understanding the problem trying to solve
  - Close the loop → RCFA drives business process improvement

ACTC: Variable Translation

- ACTC → all about data relationships among risk variables
  - Also uses FSM
  - Dependent on exploitation order of operations
    - People
    - Process
    - Technology
    - Exploitative work
- ACTC designed to
  - Characterize threat data consistently
  - Clarify how threat relates to and affects risk
  - Help people consume threat intelligence
  - Derive threat intelligence from R = P x I data
  - Move data more easily among groups without restriction

Project Status

- Project status
  - Work is just now kicking off
  - Will be using an agile development cycle
    - Reality management
    - Deliverable form and function
    - Consumer needs/requirements
  - Have industry partners onboard
- Volunteerism and reciprocity
  - Reality management volunteers needed
  - ROI → 2 for 1 deal

Questions??????

- No questions = unsuccessful presentation
- Unsuccessful presentation = lack of volunteers/industry participation
- Lack of industry participation = program failure

Contact Information

DOE-OE Program Sponsor: Carol Hawke

INL Program Managers: Dave Kuipers & Rita Wells

Bri Rolston

Critical Infrastructure Security Analyst

National & Homeland Security

Idaho National Laboratory

(208) 526-0026, office

Bri . Rolston @ inl . gov