Developing a Cyber Incident Communication Management Exercise for CI Stakeholders

Tomomi Aoyama, Kenji Watanabe, Ichiro Koshijima, and Yoshihiro Hashimoto

Nagoya Institute of Technology, Japan
Today’s topic

Background
- Types of cyber security training
- Current Trends in Japanese ICS security training

Industrial Control Systems (ICS) security exercise @NIT
- Contents
- Results from the pilot exercise
Mapping cyber security exercise
Example: large-scale adversarial exercise

- Awareness
- Hard skill (Technical)
- Soft skill (non-technical)

Prevention:
- Game
- Seminar

Response:
- Drill

Drill:
- Exercise (Table top)
- Large-scale adversarial exercise

Example: large-scale adversarial exercise
Mapping cyber security exercise
ICS security exercise in Japan

Characteristics:
- Lecture style is preferred than discussion style
- Participation is restricted to certain expertise profiles or CI sectors

Awareness

Hard skill
(Technical)

Soft skill
(non-technical)

Prevention

Response

Kaspersky Card Game

CSSC Drill

JPCERT/CC APT Training

NISC Exercise
ICS security exercise @NIT

Scope

Focus on soft skill
• Table top exercise
• Highlight the importance of communication and cooperation

Allow knowledge transfer across sectors
• Discussion based exercise
• Open to participants from all expertise profiles and CI sectors
ICS security exercise @NIT

Scenario

Cyber incident within a simplified organization structure (community heating/cooling facility)
ICS security exercise @NIT

Plan

Briefing
- Introduction of the exercise: rules, general scene description (system configuration, organization structure, etc.)
- Share the goal and the expected outcome of the exercise

Scene description
1st Cycle
The disruptive event / First response
2nd Cycle
Preparation for recovery
3rd Cycle
Recovery

Group work
- Create a workflow on the worksheet (who / what / when)
- Explore various aspect of the situation

Discussion
- Experience Sharing: Presentation by each group, comments by advisors

Debriefing
- Review the whole exercise : Establish a common takeaway
- Evaluate the exercise (not the participants): Achievement of the goal, Comprehensibility of the scenario and the exercise system
ICS security exercise @NIT
Group-work Output

- Create a work flow of actions
- Visualize communication structure
ICS security exercise @NIT
Administration

- Replier
  - Scenario injection
  - Reply questions
  - Enrich scenario detail

- Advisor
  - Technical advisor
  - Support team discussion

- Group of Participants
- Facilitator
  - Scene description
  - Time management
  - Lead discussion
ICS security exercise @NIT
Two pilot exercises

- August 2015
  - 45 participants
- March 2016
  - 46 participants

Sectors of CI owners include:
- chemical
- energy
- gas
- telecommunication
ICS security exercise @NIT
Variation of communication structure
ICS security exercise @NIT

What we learned

• Exercise was general enough to stimulate the discussion among participants with any backgrounds
• Most organizations in the ICS field are not endowed with a tailored cyber incident procedure yet
• The exercise was appreciated as an unique networking opportunity

Future work: develop a role-playing exercise to simulate the effect of possible communication management structures