Red Team vs Blue Team Tabletop Exercise and Random Scenario Creation Using Cards

Yoshihiro Masuda (Fuji Xerox Co., Ltd.)
Mitsuru Haba (Canon Inc.)
Chiyuki Matsuda (DeNA Co., Ltd.)
Yusuke Kon (Trend Micro Inc.)
Takashi Kikuta (transcosmos Inc.)
Satoshi Yamaguchi (NTT Co.)

FIRST™
Improving Security Together

Agenda

13:45-14:00 Introduction

14:00-15:10 Hands-on: Tabletop Exercise

- ✓ Procedure explanation
- ✓ Self-introduction & role assignment (blue & red)
- ✓ Briefing on incident handling procedure(blue-team) & scenario developing (red-team)
- ✓ Executing the exercise
- ✓ Review

15:10-15:15 Closing Remarks

Introduction

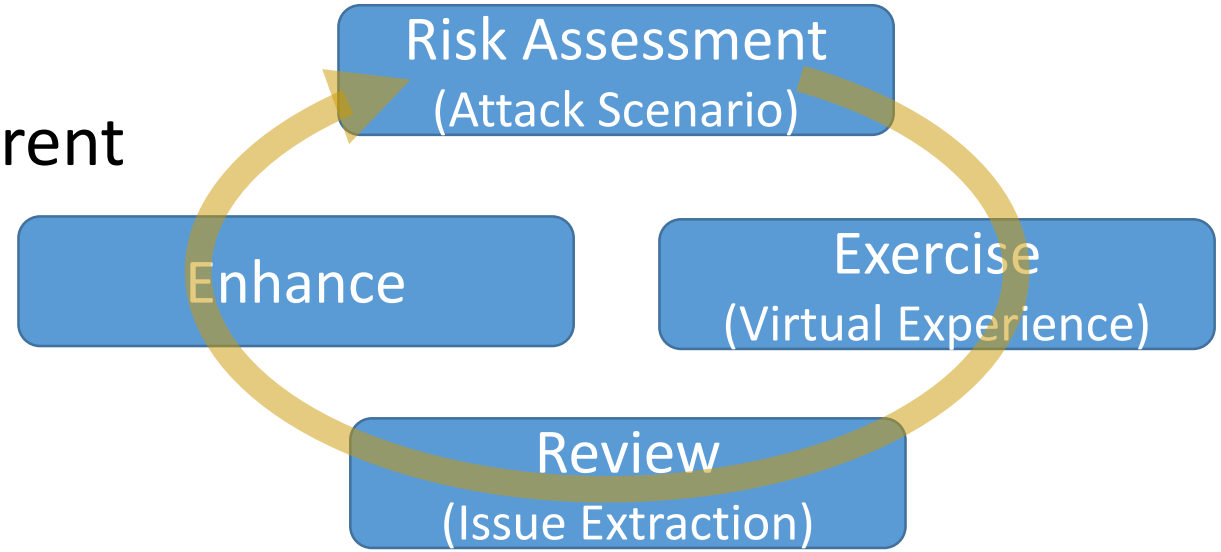
Why Exercising is Required for CSIRTs?

A CSIRT can most easily be described by analogy with a fire department.

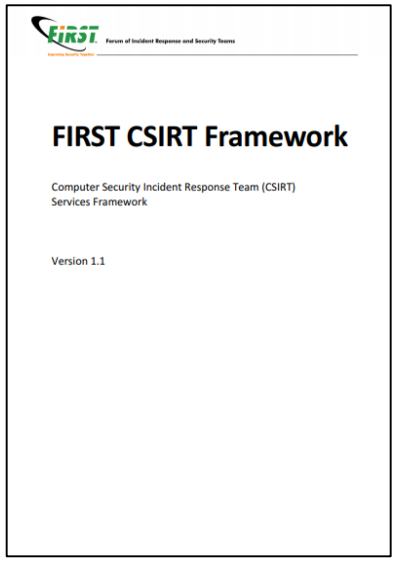
– Handbook of CSIRTs, CMU

Purpose of exercise

- Become mentally ready for cyber attacks and familiar with incident handling procedure
- Extract issues and problems on current incident handling procedure and environment
- Improve incident handling manual



Conducting Exercises is a Required Capability for CSIRTs



FIRST CSIRT Service Framework 1.1

Service Area 6 Capability Development

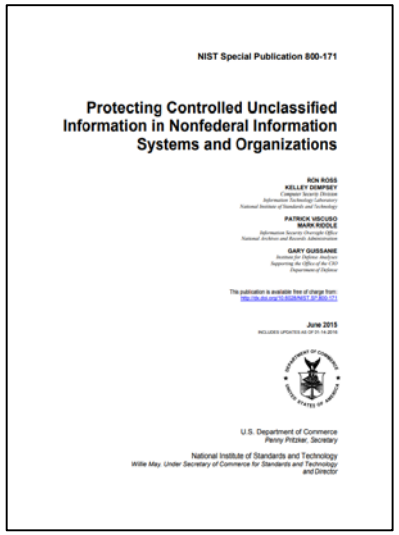
6.3 Service - Conducting Exercises

6.3.1 Function - Format and Environment Development

6.3.2 Function - Scenario Development

6.3.3 Function - Executing Exercises

6.3.4 Function - Exercise Outcome Review



NIST SP800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

3.2 AWARENESS AND TRAINING

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

But, Half of CSIRTs have No Experience on Exercises

A survey conducted in 2016(*) says, almost half of CSIRTs have no experience on incident response exercise.

Do you have an experience on incident response exercise?
Yes - United States: 39.4%, Europe: 34.7%, Japan: 33.4%

(*) http://www.ipa.go.jp/security/fy27/reports/ciso-csirt/index.html

Which Exercise Method Solves the Issues?

Types of Exercise Method

Category	Method	Execution Cost	Use Real Environment?	Procedure and Actions	Use Possible Scenario?
Discussion-based Exercises	Seminars	Low	No	Predefined	Yes
	Workshops	Low	No	Predefined	Yes
	Tabletop Exercises (TTX)	**Low**	**No**	**Resilient**	**Yes**
	Board Games	Low	No	Resilient	No
Operation-based Exercises	Drills	Medium	Yes	Predefined	Yes
	Functional Exercises	High	Yes	Predefined	Yes
	Full-Scale Exercises	High	Yes	Predefined	Yes
	Cyber Range	High	Yes	Resilient	No

Tabletop exercise (TTX) seems comparatively light-weight, and effective way to train resiliency at emergent situation

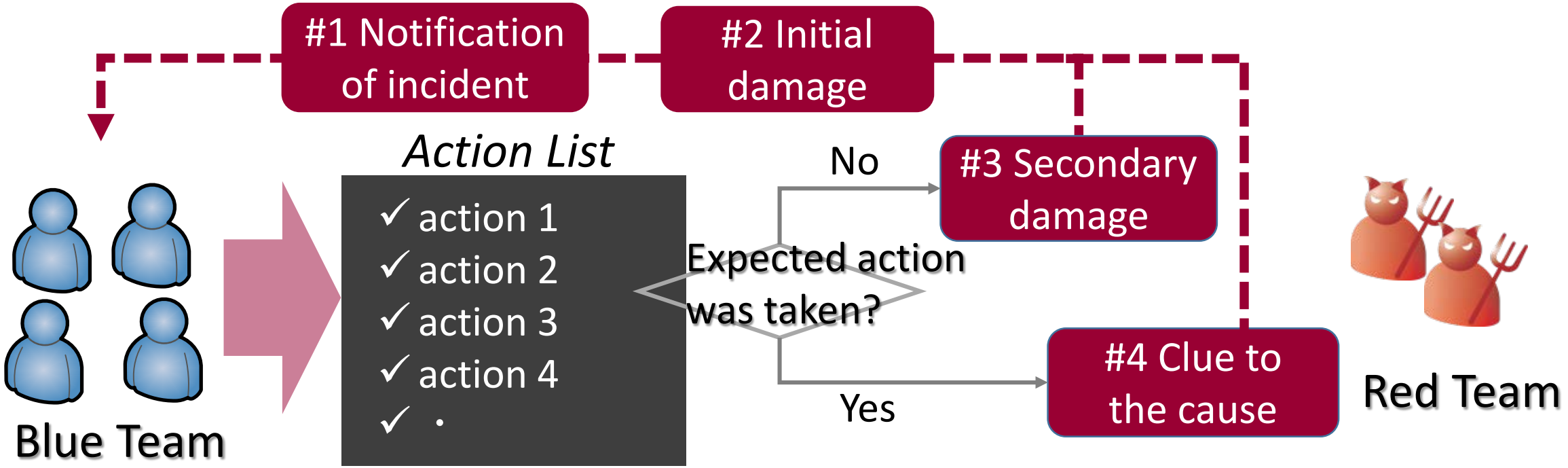
Incident Response Exercising Working Group of Nippon CSIRT Association, Japan

- Started on April, 2016
- Almost 70 CSIRTs in Japan
- Regular meeting (quarterly):
  - ➢ Sharing experiences of exercise at members' CISRT
  - ➢ Execution of tabletop exercise
- Output:
  - Guide for executing tabletop exercise
  - Tabletop exercising toolset

Features of Our Tabletop Exercising Method (1 of 2)

Feature 1: Blue team vs Red team Exercise

Making up for the lack of facilitation skills



Evaluation

1. Secondary damage was prevented ?
2. Cause of the incident was identified ?

Features of Our Tabletop Exercising Method (2 of 2)

Feature 2: Random Scenario Creation with Cards

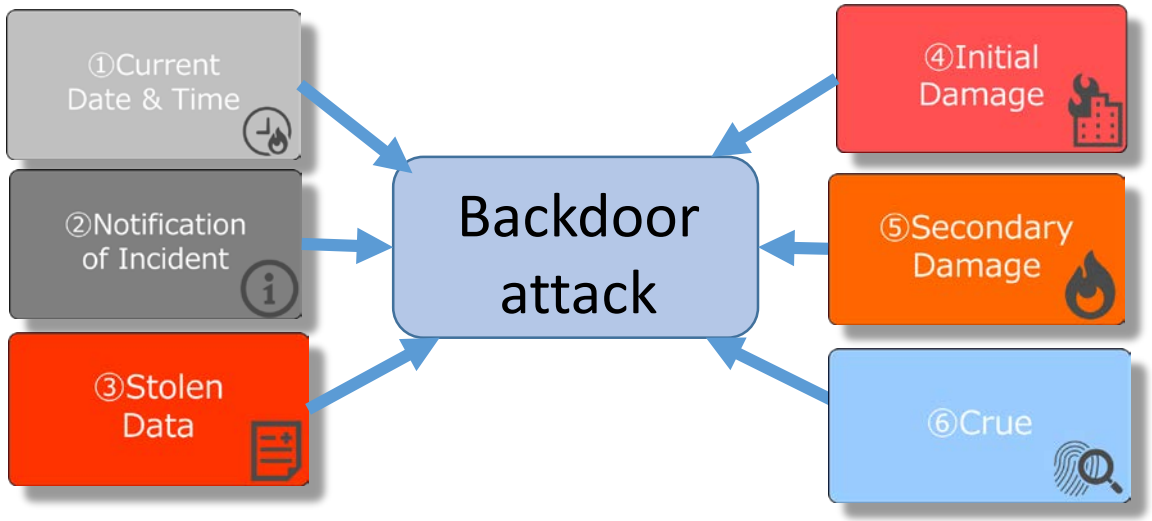
Making easy to develop exercising scenario and save preparation time

Step 1 Select a base scenario

Base Scenarios

- ☐ Zero-day attack
- ☑ Backdoor attack
- ☐ Internal fraud

Step 2 Select surrounding conditions with cards



Step 3 Improvise the scenario at execution of the exercise

Hands-on:
Tabletop Exercise

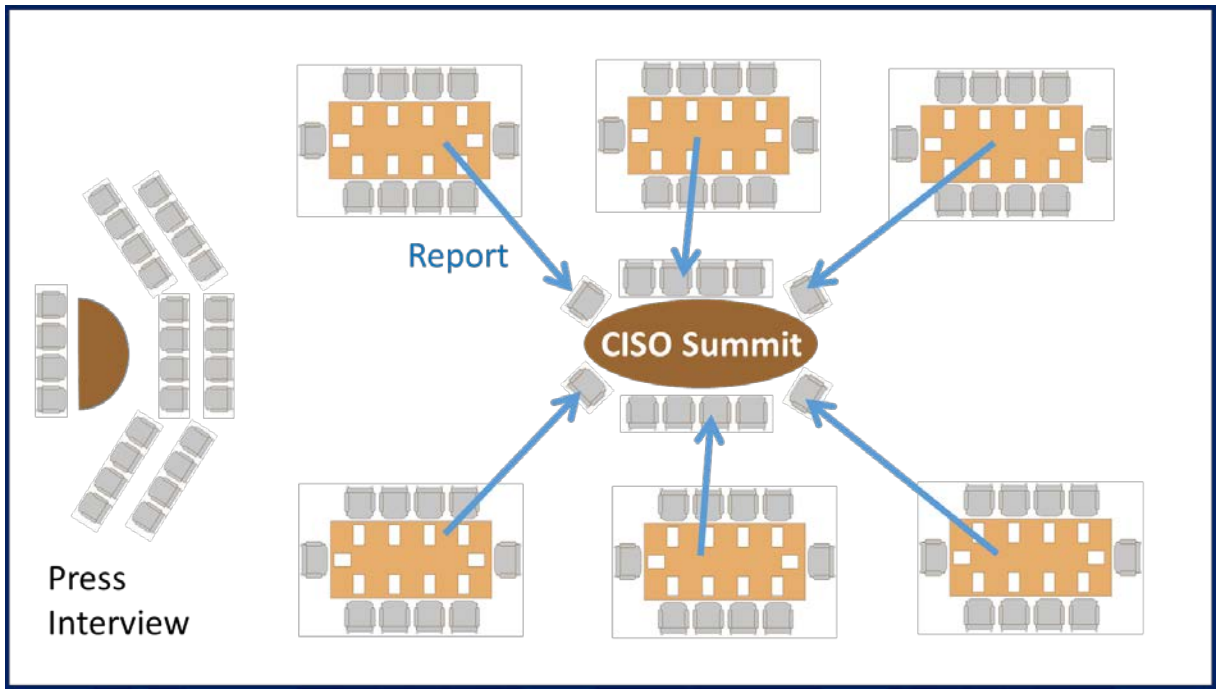
Closing Remarks

Expected Effects of Our Tabletop Exercising Method

Feature	Expected effects brought by the feature
Blue team vs red team exercise	• Skilled facilitator is not required • Enforces red team members to think as an attacker
Random Scenario Creation using cards	• Easy to develop an exercising scenario • Save time for developing an exercising scenario

An Example: Application at Workshop Seminar

- Optional training at TRANSITS Workshop in Japan
- Introduced an actor of CISO and trained about,
  - ✓Reporting to busy CISO – CISO is in the CISO Summit
  - ✓Press interview – CISO must achieve their accountability



Future Works

- Sample scenario enhancement based on case study of real incidents
- Introducing log analysis and timeline concept

- The TTX toolset is provided for free
  Please contact: nca-drilling-wg-owner@nca.gr.jp

Thank you!