Development on Guidance of Cyber Security Exercise for the Nuclear Facilities

Hyundoo Kim[*]
Korea Institute of Nuclear Nonproliferation and Control (KINAC), 1534 Yuseong-daero, Yuseong-gu, Daejeon, Korea
[*]Corresponding author: hdkim@kinac.re.kr

1. Introduction

Cyber threats and attacks are increasing rapidly against infrastructure including energy and utilities industry over the world. Because of lack of human resource and incident response system to prevent or defend increased cyber threats, many governments and major national infrastructures perform cyber security exercises to improve capabilities of cyber security incident response.[1][2] Accordingly there are exponential growth in the number of cyber security exercises over the past decade with the trend expecting to accelerate in the coming years.[3]

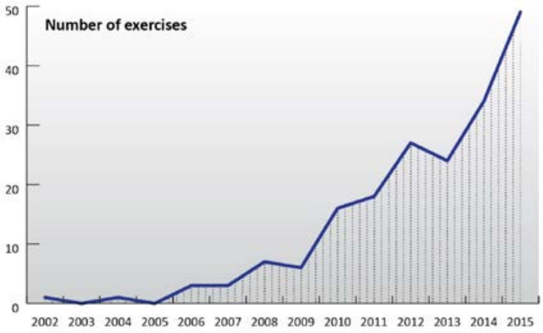

Fig. 1. Number of exercises between the years 2002-2015[3]

During the past three years almost half of the cyber security exercises reported were one off exercises the other half were part of recurring series. This report means that many exercises are regularly conducted to achieve the goals.[3]

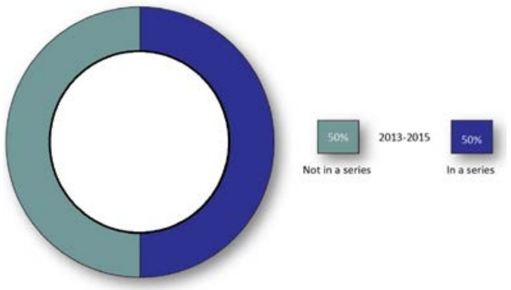

Fig. 2. Exercises in a series[3]

2. Overseas Cyber Security Exercises

The Netherlands' National Coordinator for Counterterrorism and Security (NCTV) designed and conducted @tomic 2012 international tabletop exercise to test the international response for radiological and nuclear security with cyber aspect. The following exercise @tomic 2014 was attended by over 250 governmental experts from 50 countries.[4][5]

The Government Security Operation Coordination (GSOC) team under Japan's National Information Security Center planned and held a large scale-cyber exercise called '3.18 cyber training' which was participated from the 21 governmental ministries and agencies and critical infrastructure industry such as airlines, electronic power, finance, gas, water supply and railway. This exercise is held annually in Japan.[6]

The Asia Pacific Computer Emergency Response Team (APCERT) conducts its annual drill to test the response capability of leading Computer Security Incident Response Teams (CSIRT). Throughout the exercise, the participating teams which are from over 20 countries including Korea test their incident response handing arrangement and enhance international cooperation.[7]

3. Domestic Cyber Security Exercises

The National Intelligence Service (NIS) plans exercise to evaluate response capabilities of information and Communications infrastructures such as airport, harbor, railway, traffic control, gas and electronic power against cyber attacks on control systems. This exercise focuses on a quick report of each exercise step for response of national security dimension.

In addition, there are many exercises led by governmental department or Korea Internet and Security Agency (KISA).

4. Development on Guidance of Cyber Security Exercise

Act on Physical Protection and Radiological Emergency (APPRE), its Enforcement Regulation and its Notice require licensees of Nuclear Facility to conduct physical protection exercise including cyber security exercise to respond and mitigate effects of nuclear terrorism.

Those legislations were amended on 2014. Licensees had a grace period by 2015 and conducted or will conduct cyber security exercise on 2016.

4.1. Establishment of Goals

According to the research study, most exercises were designed to focus on training the participants, and provide an opportunity to gain knowledge, understanding and skills. This particular exercise design represents a 47% of the cyber security exercises. Another exercises were designed to focus on developing activities, abilities and ideas that represents 31% of the exercises.[3]

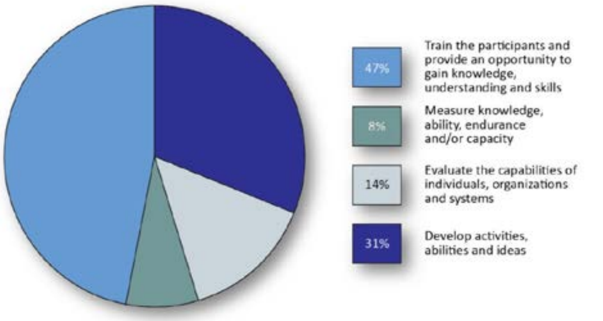

Fig. 3. Exercise design[3]

Based on this study, goals for cyber security exercise were established after discussion with licensees. The goals are followed:

- Train participants and provide an opportunity
- Check necessity of new incident response systems
- Evaluate capabilities of existing incident response systems

4.2. Set-up of Steps

The guidance of procedures of incident response written by KISA classified the procedures into five(5) steps: detection, initial response, establishment of strategy, investigation and restoration.[8]

Because the nuclear facilities have specific characteristics which are prevention of radioactivity proliferation and mitigation of accident, the seven(7) steps of cyber security exercise for the facilities were set up. The seven(7) steps are followed:

- Detection of cyber attack
- Initial response
- Organization of cyber incident response team
- Notification and report
- Collection of evidence
- Analysis
- Elimination and restoration

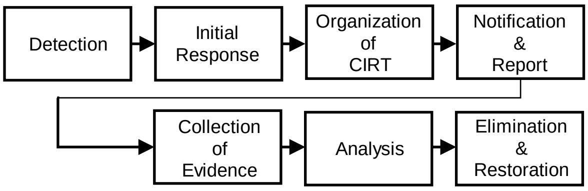

Fig. 4. Steps of cyber security exercise

4.3. Selection of object system

The systems of Nuclear Facility are classified as control system, security system and emergency preparedness system. 2016 cyber security exercise was first exercise which focused on mitigation and recovery of cyber incident. And to interconnect with physical protection exercise security system was selected as object system in 2016 cyber security exercise.

4.4. Scenario

The scenario of cyber security exercise was developed within the Design Basis Threat (DBT) which was reset in 2015.

4.5. Actual Exercise vs Tabletop Exercise

The licensee tried to increase the portion of actual exercise as much as possible. However situations such as absence of the procedure and connection with other government agency or organization were conducted by tabletop exercise.

5. Conclusions

Even though there were many cyber security exercises in the Nuclear Facilities, this exercise was first which focused on mitigation and recovery of the system of the Nuclear Facility against cyber incident.

So many insufficient items were deduced such as absence of a procedure for mitigation and recovery of cyber incident. These procedures should be developed and established through 3rd phase of Cyber Security Plan (CSP) and other technical complement actions under regulatory body's guidance.

Also developed and existed procedures should be regularly performed to make cyber incident response team and related people rapidly response against cyber incident through exercises or other trainings. The insufficient items come from the exercise should be reflected to developed and existed procedures by periods.

In addition, the portion of actual exercise instead of tabletop exercise should be extended to meet the goals and make useful training for the participants. Various scenario such that safety system which causes adverse effect to nuclear facilities is selected as target system should be developed to make diverse opportunity and many participants.

REFERENCES

[1] "Cisco 2014 Annual Security Report", CISCO, 2014
[2] Internet & Security Bimonthly 5th, KISA, 2015
[3] "The 2015 Report on National and International Cyber Security Exercises", enisa, 2015

[4] “@tomin 2012: An Exercise in Perspective”, NCTV, 2013

[5] unicri web site: http://www.unicri.ir/news/article/

[6] Internet & Security Bimonthly 2nd, KISA, 2015

[7] “APCERT EMBARKS ON CYBER ATTACKS BEYOND TRADITIONAL SOURCES”, APCERT, 2015

[8] “The guidance of procedures of incident response”, KISA, 2010