Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 27-28, 2016

Study on Nuclear Facility Cyber Security Awareness and Training Programs

Jung-Woon Lee[*], Jae-Gu Song, Cheol-Kwon Lee
I&C and Human Factors Research Division, Korea Atomic Energy Research Institute, Daejeon, Republic of Korea
[*]*Corresponding author: leejw@kaeri.re.kr*

1. Introduction

Digital technologies have been applied expansively to nuclear instrumentation and control systems. This application has raised concerns on cyber security. Korea Institute of Nuclear Nonproliferation and Control (KINAC) issued the regulatory standard RS-015[1] in 2014 and asked Korean nuclear facilities to submit a cyber security plan (CSP) and to implement the CSP according to the seven step schedule.

Cyber security awareness and training, which is a part of operational security controls, is defined to be implemented later in the CSP implementation schedule. However, cyber security awareness and training is a prerequisite for the appropriate implementation of a cyber security program. When considering the current situation in which it is just started to define cyber security activities and to assign personnel who has responsibilities for performing those activities, a cyber security awareness program is necessary to enhance cyber security culture for the facility personnel to participate positively in cyber security activities. Also before the implementation of stepwise CSP, suitable education and training should be provided to both cyber security teams (CST) and facility personnel who should participate in the implementation.

Since such importance and urgency of cyber security awareness and training is underestimated at present, the types, trainees, contents, and development strategies of cyber security awareness and training programs are studied to help Korean nuclear facilities to perform cyber security activities more effectively [2].

2. Types of cyber security training and trainees

Cyber security awareness and training is described in Appendix 1 of RS-015 as a part of operational security controls. Three types of cyber security awareness and training, which are 1) awareness training, 2) technical training, and 3) specialized cyber security training, are addressed. Also in the cyber security incident response and recovery section in RS-015, ‘incident response training,’ ‘incident recovery plan review and training,’ and ‘incident recovery education’ are mentioned. These training and education can be categorized as 4) incident response and recovery training. As results, the four types of training programs are identified.

Cyber security awareness training should be provided to all the facility personnel including contractors. In the description of technical training, two groups are mentioned. One is ‘individuals that are involved in the design, modification, and maintenance of critical digital assets (CDAs), and the other is ‘system managers, cyber security specialists, system owners, network administrators, and other personnel having access to system-level software.’ These two groups can be called as system engineers. This technical training is also provided to the members of cyber security team (CST), who are individuals that have cyber security responsibilities related to programs, processes, and procedures. For specialized cyber security training, CST and cyber security incident response team (CSIRT) become trainees. Table I shows the types of cyber security training and trainees.

Table I. Types of cyber security training and trainees

Types of cyber security training	Trainees
1. Awareness Training	All employees and contractors
2. Technical Training	System Engineers and CST
3. Specialized Cyber Security Training	CST and CSIRT
4. Incident Response and Recovery Training	CSIRT and System Engineers

3. Contents of cyber security awareness program

Items to be included in a cyber security awareness program are collected from the requirements in RS-015 and listed as follows;

- updates on new threats and technology
- assigned roles and responsibilities
- specific requirements identified by the defensive strategy
- CDAs to which personnel have authorized access
- the site-specific objectives, management expectations, programmatic authority, roles and responsibilities, policies, procedures, and consequences for noncompliance with the cyber security program
- general attack methodologies, including social engineering techniques and appropriate and inappropriate cyber security practices
- organizational contacts to whom to report suspicious activity, incidents, and violations of cyber security policies, procedures, or practices
- an explanation as to why access and control methods are required
- measures users can employ to reduce risks
- the impact on the organization if the control methods are not incorporated

By interpreting these items, the following items are devised in this study as contents of a cyber security awareness program;

1) General cyber threats. methods, attack techniques
(including new threats and techniques, if any)
2) Cyber attack cases with attack methods and consequences (in nuclear or industrial control systems (ICS))
3) Meaning of CIA(confidentiality, integrity, availability) and potential risks from compromising CIA
4) Five attack vectors (network, wireless, portable media and mobile devices, supply chain, and physical access)
5) Introduction : Elements of CSP
   - purpose,
   - the scope of protection,
   - the cyber security team,
   - asset identification and analysis,
   - defense-in-depth strategy,
   - assessment of compliance with the requirements of cyber security controls,
   - implementation of technical, operational, and management security controls,
   - continuous monitoring and assessment, and
   - change control

   (if site-specific cyber security guides and procedures are developed, include the contents of these documents)
6) Introduction : technical, operational, and management security controls of RS-015
   - policies, or brief requirements,
   - the impact on the organization if the control methods are not incorporated
7) Organizational contacts to whom to report suspicious activity, incidents, and violations of cyber security policies, procedures, or practices (introduce attack indicators and reporting system)
8) Terminologies other than those mentioned above

4. Contents of technical training

Technical training helps plant system engineers and CST to perform suitably the cyber security activities defined in the CSP. Cyber security activities in CSP can be identified as follows;

1) Identification of critical systems (CS) and critical digital assets (CDAs)
2) Security level assignment under the defense-in-depth(D-i-D) strategy
3) Assessment of CDAs' compliance with security control requirements in RS-015
4) Application of required security controls
5) Performing cyber security activities related to CDAs after the implementation of security controls
   - the operation of technical security controls
   - the operation of operational and management security controls
6) Change control
7) Supports for cyber security incident response
   - Incident handling
   - Incident monitoring
   - CDA backups
   - Recovery and reconstitution, etc.

Among these, training for the activity 7) can be included in '4. Incident Response and Recovery Training.' For the other activities, contents are developed as in Table III.

Table III. Contents of technical training

Cyber security activities	Contents of technical training
1) CS and CDA identification	- Definition of CS and CDAs - Methods and Procedures
2) D-i-D strategy	- Meaning of D-i-D strategy - Security level assignment criteria - Identification of connections violating D-i-D rules and possible solutions for those connections
3) Assessment of security control requirements	- Introduction of 101 security controls in RS-015 - Assessment methods and procedures - Criteria for the applicability of the requirements in CDAs - Criteria for compliance
4) Application of required security controls	- Methods and procedures for the selection of candidate security control designs - How to evaluate the applicability, suitability, and effectiveness of security controls
5) Activities after the implementation of security controls	- Procedures for security control operation
6) Change control	- Procedures for the change control - Methods to evaluate the cyber security effects of changes

For most of the activities, training materials should be developed based on the facility cyber security procedures. If procedures are not available, training material can be developed based on RS-015. Elements of technical training programs can be developed individually as the activities to be performed.

5. Specialized cyber security training

CST and CSIRT are the trainees of specialized cyber security training. In order for this training to be effective, the program should be developed based on the CDAs of nuclear facilities. This training program is not available now and its development needs considerable time. It is recommendable to utilize the test-bed built with CDAs in nuclear facilities for the development of a specialized cyber security training program.

ICS-related cyber security training programs being offered in foreign countries may be considered as alternatives to a specialized cyber security training program. There are SANS ICS cyber security training courses [3] and ISA cyber security training courses [4], which are highly relevant. Black Hat Conference training programs [5], Infosec Institute SCADA/ICS Security Boot Camp [6], and Cybati Control System Cybersecurity Course and Training Kit CybatiWorks™ [7] can be considered also as candidates.

6. Incident response and recovery training

Cyber security incident response plans may cover incident handling, incident monitoring, recovery, and reconfiguration. Incident response and recovery training should be developed in accordance with incident scenarios based on this incident response plan.

Research on the detection and analysis of cyber security incidents in nuclear facilities should be performed to make more feasible incident response plans. It is necessary to develop incident response and recovery training programs as the incident response plans are updated.

7. Conclusion

Cyber security awareness and training programs should be developed ahead of the implementation of CSP. In this study, through the analysis of requirements in the regulatory standard RS-015, the types and trainees of overall cyber security training programs in nuclear facilities are identified.

Contents suitable for a cyber security awareness program and a technical training program are derived. It is suggested to develop stepwise the program contents in accordance with the development of policies, guides, and procedures as parts of the facility cyber security program. It is also suggested to develop technical training programs suitably for the performance of cyber security activities defined in the stepwise CSP implementation schedule.

Since any training programs are not available for the specialized cyber security training in nuclear facilities, a long-term development plan is necessary. As alternatives for the time being, several cyber security training courses for industrial control systems by foreign institutes are searched and introduced.

Incident response and recovery training programs may be developed based on the facility incident response plans. In order to have an effective incident response plan, more researches on the detection and analysis of cyber security incidents in nuclear facilities are necessary. It is suggested to update the cyber security incident response and recovery training program as incident response plans are updated.

ACKNOWLEDGMENT

This work has been supported by a grant from the Korea Ministry of Strategy and Finance.

REFERENCES

[1] KINAC/RS-015, Technical standard for the security of computer and information systems in nuclear facilities, Rev. 1, KINAC, 2014.

[2] Jung-Woon Lee, Jae-Gu Song, Cheol-Kwon Lee , A Study on the Development of Nuclear Facility Cyber Security Awareness and Training Program, KAERI/TR-6424/2016, KAERI, 2016.

[3] https://www.sans.org/course

[4] https://www.isa.org/uploadedFiles/Content/PDFs/5736_Cybersecurity-Training2016-Booklet_WEB.pdf?utm_source=brochure&utm_medium=website&utm_campaign=cyber-train-broc-page

[5] https://www.blackhat.com/us-16/training/index.html

[6] https://www.infosecinstitute.com/courses/scada-security-boot-camp

[7] https://cybati.org/education