Case Study on the Insider Threat Mitigation at Nuclear Facilities : United Kingdom and Japan

Chan Kim [a*]
[a]*Korea Institute of Nuclear Nonproliferation and Control(KINAC)*
1418 Yuseong-daero, Yuseong-gu, Daejeon 34101
[*]*Corresponding author: ckim@kinac.re.kr*

1. Introduction

The international community, including the IAEA, defines that the malicious behavior of insiders at nuclear power plants is the most fatal illegal activity for the establishment of an international physical protection system. Accordingly, the IAEA has developed and published the document INFCIRC/908 for reducing insider threats and is seeking future countermeasures with an international group of experts through holding an international symposium. In addition, in order to solidify the international physical protection system on this issue, the IAEA strongly recommends to encourage member states to sign the document and to strengthen measures to mitigate insider threats in their own country. [1]

This study examines international norms and foreign cases directly related to insider threat reduction, and discusses factors that can be referred to in the current status of domestic insider reduction measures.

2. IAEA Guideline

2.1 Nuclear Security Series No.8 and No.8-G(Rev.1)

In NSS No.8 “Preventive and Protective Measures against Insider Threat”, IAEA defines Adversary as outsider and insider as targets of harm to nuclear power plants. In particular, insiders are those who have access to nuclear power plants and related facilities due to their positions and access authority, they can determine the best time for penetration of the facility and weaknesses of it. The exercise of their malicious intentions and actions can cause fatal adverse effects on nuclear facilities. Hence, the IAEA has developed this document to provide general guidance to its national protection agencies and facility operators to ensure that member states implement proactive and protective measures against insider threats. In addition, the IAEA recommends that the international physical protection guideline, INFCIRC/225/Rev.4, the physical protection technical guideline TECDOC-967, and TECDOC-1276 should be applied together. [2,3]

2.2 INFCIRC/908

In December 2016, the United States requested circulation to the IAEA Secretariat through diplomatic documents for 29 IAEA member states including INTERPOL for the purpose of raising awareness and setting up practical countermeasures to insider threats. Accordingly, the IAEA strongly requested member states to establish and implement measures at the state-level to mitigate insider threats in nuclear facilities, and the main contents are as follows. [4]

1. Member States support the IAEA to develop and implement practical training courses for the prevention and protective measures of insider threats.
2. Member States shall implement one or more of the following measures:
   - Development and implementation of national policies for mitigation of insider threats
   - Develop and maintain results-based regulatory system approaches
   - Promote cooperation between national agencies and establish special steps to share information
   - Establishment and reinforcement of a regulatory system related to NMAC programs for nuclear security purposes
   - Establishing a protection system for nuclear materials and facilities from insider activities
   - Establishment of personal reference program for workers at nuclear facilities
   - Investigation related to drugs and alcohol

3. United Kingdom

3.1 Perspective on Insider Threat

The UK has a greater interest in insider threats than other European countries. According to the Report of Vormetric, the UK was the only country to say that the cloud computing environment was the biggest risk factor, when many countries considered data breaches as their biggest concern. This is the result of the UK's strong acceptance of cloud computing as the most viable alternative to local data storage. In addition to insider threats, the UK has a high level of concern about fraud and theft of personal information. According to a Vormetric survey, more than 40% of UK businesses believe that privileged users, such as system/DB/network administrators, may be the biggest threat to their organization.

However, things like data breaches and cloud computing environments are not the only insider threats that the UK considers. Factors such as the digital environment are evaluated relatively less, while those

such as terrorist-based insider incidents appear to be considered more. In recent years, the UK has raised the level of insider threats related to terrorists due to the increasing number of British Muslims joining groups such as ISIS [5].

3.2 CPNI's Insider Threat Mitigation Framework

The Center for Protection of National Infrastructure is a UK government authority under the Director General of MI5 for protective security advice to the UK national infrastructure. The role of CPNI is to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats. [6]

CPNI has reviewed and analyzed cases of insider acts from the UK and overseas to understand how and why these events occurred, and what could have been done to prevent them. The Insider Data Collection Study report provides CPNI's main findings. CPNI has used this data to test, refine and embed personnel security into protective measures. [7]

The insider threat mitigation system suggested by CPNI is as follows.

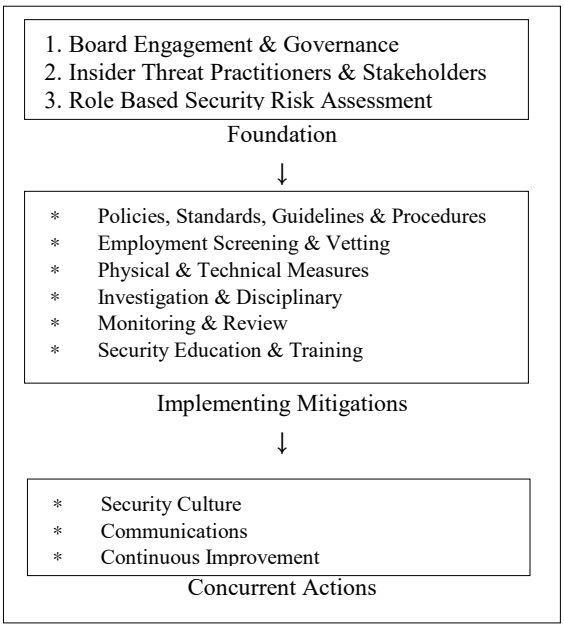

Fig1. CPNI's Insider Mitigation Framework [8]

4. Japan

4.1 Perspective on Insider Threat

Japan is generally known as largely heterogeneous and peer pressure is quite high, meaning that Japanese organizations tend to default to trust. As a result, Japan is a remarkable exception to the widely accepted norm that privileged users are the group that poses the greatest threat to an enterprise [9]. According to the Vormetric Report, Japanese believed that average users (56%) would be the biggest threat. In addition, Contractors and Service Providers ranked second with a slight margin of 52%, and privileged users with a low percentage of about 37% [10]. The underlying reason for this difference likely lies in Japanese culture itself, which fosters a belief that employees are loyal and trustworthy by nature and that insider threat activities are unthinkable [9].

4.2 NMCC

It is known that Japan has established and implemented mid- to long-term plans to find practical countermeasures, including countermeasures against insider threats for more than 10 years, under the supervision of the Nuclear Material Control Center (NMCC) [11]. NMCC investigated overseas cases as part of a research for countermeasure to insider threats, related to nuclear material protection. Based on that results, the working group including the business operator organized basic concepts such as insider definitions and countermeasures, and establishes survey items for nuclear facilities in Japan. Field surveys were preceded and countermeasures were established and reviewed. To establish Design Based Threats, in-depth investigations were conducted on the evaluation of the physical protection system, analysis and evaluation of threats, indoor and field tests of the protection facilities, and response measures in case of emergency protection over the past 10 years. In addition, in accordance with the request of JAEA in 2019, an international training course for the mitigation of insider threats under the supervision of the IAEA was held to devise practical measures. Since then, JAEA has developed its own training program to reduce insider threats. And currently, in order to raise awareness on insider threats and to strengthen countermeasures for its nuclear business operators, Japan is running five educational programs every year [1].

5. Conclusion

Korea has enacted and implemented the "Act on Protection and Prevention of Radiation Disaster for Nuclear Facilities" in 2004 to reinforce and re-establish the physical protection system for nuclear power plants since the 9/11 terrorist incident. In addition, since the Design Based Threat(DBT) was established in 2009 for the first time in accordance with the same Act, the DBT has been revised for the fourth time in 2018 to strengthen the physical protection system for nuclear power plants.

In order to establish and implement a system for responding to insider threats systematically, as in the case of other countries, it is inevitable to change the level of awareness, that is, to enhance the nuclear security culture. This is because the establishment and

implementation of a system alone that does not accompany communication/security culture/continuous improvement, as can be seen in the diagram of the UK CPNI's insider threat mitigation framework, will be ineffective.

Lastly, in order to reduce insider threats in the field, in-depth research on insiders and development of personnel security enhancement programs should be accompanied.

REFERENCES

[1] Jong-Uk Lee, KINAC/OT-007/2019, Oversea Report on 2019 International Symposium on Insider Threat Mitigation, March, 2019.
[2] Nuclear Security Series No.8, "Preventive and Protective Measures against Insider Threats", Implementing Guide, IAEA, 2008.
[3] IAEA Nuclear Security Series No. 8-G(Rev.1), Implementing Guide, "Preventive and Protective Measures against Insider Threats", 2020.
[4] INFCIRC/908, Joint Statement on Mitigating Insider Threats, Communication dated 22 Dec. 2016 received from the Permanent Mission of the United States of America concerning a Joint Statement on Mitigating Insider Threats, 2017.
[5] Mehan, Julie E. Chapter 5. Regional Perspectives on Insider Threat, "Insider Threat: A Guide to Understanding, Detecting, and Defending Against the Enemy from within", IT Governance Pub, 2016, pp.109
[6] Centre for the Protection of National Infrastructure. *About*. 2020. https://www.cpni.gov.uk/about.
[7] Centre for the Protection of National Infrastructure. *Reducing Insider Risk*. 13 Oct 2020. https://www.cpni.gov.uk/reducing-insider-risk.
[8] Centre for the Protection of National Infrastructure. *Insider Risk Mitigation Framework*. 21 May 2019. https://www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework.
[9] Mehan, Julie E. Chapter 5. Regional Perspectives on Insider Threat, "Insider Threat: A Guide to Understanding, Detecting, and Defending Against the Enemy from within", IT Governance Pub, 2016, pp.110
[10] Vormetric, Inc. 2015 Vormetric Insider Threat Report Global Edition. 2015. p.14
[11] 일본 대형재처리시설 핵물질방호 체계 확립조사 사업계획서, NMCC, 1997.