Enhancement of Incident Handling Capabilities by Cyber Exercise

YANO Yukiko, ITO Atsushi, FUNAKOSHI Takeo, SATO Kazuyo

Abstract

Under the intensification of threats of cyberattacks the refinement of human resources capable of handling them has become a pressing issue. NEC has been studying the skills expected from such human resources and the method of handling an actual cyberattack and thereby developing an effective training program. This paper introduces the concept of NEC in developing the practical cybersecurity exercises that are currently providing training courses, together with some actual cases.

Keywords

Capacity building, cyber exercise, incident response, incident handling, cyberattack, CSIRT

1. Introduction

Since cyberattacks have spread significantly, shortages of human security resources in enterprises and organizations have now become a serious problem, thereby causing threats to information assets and business continuity. In addition, the dissemination of smartphones, social media and IoT has meant that the knowledge and capability required of security-involved people is more complex than ever.

The trend in the shortage of human security resources is a worldwide problem and serious security incidents such as falsifications of governmental websites are occurring in various countries such as in Japan. This has made the demand for the cultivation of human resources capable of dealing with such problems higher than ever.

In this paper, we define the skills required of human resources to deal optimally with the threats of cyber-attacks, describe the development of the training exercise program for strengthening such resources and introduce cases of projects that we have actually completed in Japan and in the ASEAN countries.

2. Types of Human Security Resources to be Development

This section discusses those human resources that are required to deal optimally with cyber-attack threats.

2.1 In-house CSIRT and Capacity Building

Enterprises and organizations are positively advancing the introduction of security appliances such as firewalls and IPSs in order to combat cyber-attacks.

Training for the operators of security systems consists not only of that based on programs provided by the product manufacturers. SI vendors also provide a wide variety and number of programs that contribute to the upgrading of technical skills. However, technical skills are not adequate by themselves for optimally responding to the escalating cyber-attacks. Based on these circumstances, many organizations are starting to prepare CSIRTs (Computer Security Incident Response Teams). The CSIRT is a team for undertaking the integrated handling of security incidents. The concentration of points of contact related to information security is also expected to facilitate collaborations with external organizations (**Fig. 1**).

2.2 Summary of Human Resources Required for CSIRT

In case a cyber-security event occurs, the CSIRT is required not only to clarify the occurring event and prevent any extension of damage but also to ensure continuity of the activities of the organization to which it belongs.

To maintain the activities of the organization, it is necessary to identify a situation from a higher perspective, make accurate decision on the actions to be prioritized and perform the response in as short a time as possible.

This cannot be executed with the technical skills for applying measures to the system alone. High relational skills such as the ability to make decisions, perform coordination with related departments within the organization and communication with external organizations (**Fig. 2**).

While the expectations for CSIRT have grown greatly, many barriers still exist before CSIRT members will benefit significantly. Such as the few opportunities that occur for experiencing a real incident and because of its high dependence on individual skills, the difficulty of teaching the requisite expertise to others.

●**Integration of points of contact and information** in case of incidents

- •Inter-departmental coordination (horizontal & vertical) in case multiple departments become involved
- •Points of contact for notices from outside of the organization, encouragement of other organizations

●Accumulation of **response expertise**

- •Need for preparation, considering the spread and modification of the advancement of the means of attack
- •Increase in experience for enabling a surer response

●Building of confidence for **external organizations**

- •Collaborations with external organizations through forums such as FIRST and APCERT

Fig. 1 Advantages of CSIRT.

In addition to technical skills, the members of CSIRT are required of high interpersonal skills such as the ability to communicate with the staffs of other teams as well as other with members of the team.

Type	Outline of skills
Interpersonal skills	· Common sense in making efficient and acceptable decisions whenever there is no clear ruling available and under stress or severe time constraints · **Effective oral and written communication skills to interact with constituents and other teams** · Ability to follow policies and procedures · Ability to cope with stress and work under pressure · Integrity and trustworthiness to keep a team’s reputation and standing · Willingness to continue education · **Problem solving** · **Team player** · Time management
Technical skills	· Knowledge on the Internet · Network protocols (IPv4, IPv6, ICMP, TCP, UDP) · Network infrastructure elements (router, switch, DNS, mail-server) · Network applications, services and related protocols (SMTP, HTTP, HTTPS, FTP, TELNET, SSH, IMAP, POP3) · Three basic security principles (confidentiality, integrity, availability), multilayer defense, etc. · Threats on computers and networks · Attack techniques (IP spoofing, DoS, viruses, worms, etc.) · Encryption technologies (TripleDES, AES, IDEA, RSA, DSA, MD5, SHA) · Host system security issues (backups, security patches, updating) · Programming and administration of computer systems

Source: Handbook for Computer Security Incident Response Teams (CSIRT), published by CERT/CC

Fig. 2 Skills required for CSIRT human resources.

Based on these contingency situations, NEC has decided to tackle the development of an “incident handling exercise.”

3. Outline of Incident Handling Exercise

This section introduces the outline of the “incident handling exercise” NEC has started.

NEC designed this exercise so that the trainee can learn how the CSIRT should respond to a cyberattack by experiencing it in the same time lapse as in an actual event, Technical points such as analyses as well as the factors belonging to interpersonal skills such as reporting to one’s superior and interaction with related departments and communication with external organizations will also be covered.

The incident handling exercise is a practical exercise that follows the flow of typical responses to a target attack and it also includes analyses using actual devices. Its validity has been verified after several improvements based on the results of various human resource training projects.

3.1 Goals of the Incident Handling Exercise

The following four concerns are the main goals of the incident handling exercise.

- Understanding the latest targeted attacks
- Experiencing response procedures by following attack scenarios
- Experiencing techniques and tools used in the response
- Knowledge of communications to inside and outside the organization

When the experience of the exercise is compared to situations in the trainee’s organization, the issues of the organization can be clarified and knowledge leading to improvements can be obtained. This is another of the exercise goals.

3.2 Targets of the Incident Handling Exercise

Incident handling training is given to persons in charge of information security in the information systems departments of enterprises and groups. The assumed targets are the persons who are going to start up CSIRTs or members of teams that have already started up but are not yet functioning effectively. The exercise is also very effective for persons who are going to be in charge of security operations or those that are newly joining CSIRTs.

3.3 Configuration and Mode of Provision of Incident Handling Exercise

The incident handling training consists broadly of the three subjects of "lecture," "practical exercise" and "group work" (**Fig. 3**).

The "lecture" is where the basic knowledge required for incident handling is acquired. In addition, it also provides experience of the operational environments and tools of the system used in the exercise.

"Practical exercise" is the function in which the trainees learn the flow of the incident handling sequence by controlling the actual devices in order to experience incident analyses based on actual cyberattack cases. Three to four trainees form a group and tackle the incident handling by allocating the roles of instructions, investigations/analyses and report/liaison. If a single team sends several members to the exercise, they are recommended to join the same group and experience the roles that they will actually assume in their team.

The "group work" is the place for holding discussions with the lecturers and other trainees on the strategies of each team and on the operational measures to be taken. The intention is to aim the knowledge and experience learned in the exercise at the actual operation.

Each exercise is held on two days considering the volume of the contents and adopts a group work mode to promote smooth communication between the lecture staff and the trainees and between the trainees themselves. The computers and servers used in the practical exercise are prepared by NEC.

The exercise is coordinated by a lecturer and a few tutors. The tutors support the understanding and progress of the practical exercise for the trainees. Usually, a tutor is assigned for 10 to 15 trainees.

3.4 Scenarios Used in Practical Exercise

The practical exercise is performed in a virtual environment in which the servers and networks used in real organizations are simulated. This environment allows the trainees to experience the actual flow of the incident handling (scenario) by replicating intrusion logs and malware such as the RAT (Remote Access Tool, or Remote Administration Tool). Scenarios are designed to be highly realistic by being based on actual cases of information leaks of targeted attacks.

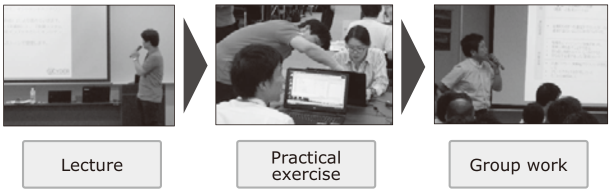

Fig. 3 Configuration of the incident handling exercise.

An example of a scenario:

(1) Notification to informant
(2) Verify the detection
(3) Alert
(4) Investigation results review
(5) Surface analysis
(6) Report of current status
(7) Investigation of damage extent
(8) Log analysis
(9) Investigation of causes of internal infection
(10) Information leakage report

To develop highly effective scenarios, the exercise incorporates advanced knowledge and the latest case histories in collaboration with academic institutions such as the Japan Advanced Institute of Science and Technology as well as partner businesses of the NEC Cyber Security Factories[1)]. The tools used in the practical exercise are selected from freeware and genuine OS items to facilitate actual introduction after the trainees return to their teams.

3.5 Effect Measurement Method

To measure if the skills of trainees have improved by receiving the training, skill check tests are conducted before and after the course in order to enable quantitative measurements by comparing the scores.

In addition to the post-exercise questionnaires, a "follow-up questionnaire" is also made experimentally at a certain period after the exercise to check the situations of trainees.

4. Enforcement of Incident Handling Exercises, Their Effects

This section introduces the summaries of training projects that NEC has been engaged in both in as well as outside Japan.

4.1 Cyber Defense Exercise with Recurrence (CYDER)

CYDER is a project started in FY2013 by the Japanese Ministry of Internal Affairs and Communications. It is targeted at governmental agencies and key infrastructure businesses and it is conducted by drawing up a scenario of incident handling against a targeted attack. The activity is expanded to meet the changes in the threats on cybersecurity and the incident handling scenarios of local governments are also developed.

The exercise has been participated by more than 2,000 trainees already. The post-exercise questionnaires reveal that the results of the training have elicited remarks such as “we started a CSIRT in our house and joined the related organization,” “we drew up an incident initial handling manual” and “we prepared the tools we used in the practical exercise so that they may also be used in-house.” This was all satisfying news for the authors and for NEC.

4.2 Cyber Exercises for ASEAN Countries

As part of the project conducted by the Japanese Ministry of Internal Affairs and Communications, “Hands-on pilot training aiming to increase cyber defense capabilities in ASEAN countries,” NEC has been presenting cyber training exercises for the governmental cybersecurity-related organizations of ASEAN countries such as Thailand and Malaysia since FY2015. These exercises are based on CYDER as described above, but the scenario contents, exercise time allocation and progress trends were adjusted according to the circumstances and national traits that were specific to each country. Although the exercise time was extended compared to CYDER in Japan, many trainees still expressed the opinion that it should have been for longer. When NEC appointed tutors speaking the local language in Thailand, noticeable improvements in results were achieved; including activation of discussions in the team exercise and group work as well as improvements in trainee understanding.

5. Conclusion

Under the continual growth of the threats of cyber-attacks, the roles of the human security resources that support the realization of a society where people can lead safe, secure lives is likely to become more important in the future.

NEC will continue to contribute to the capacity building of cyber-security resources and to their capabilities by applying the technical power and system integration expertise that we have developed.

Reference

1) Y. YANO, et al.: “Cyber Security Factory - Our Commitment to Help Developing More Effective Methods of Coping with Today’s Increasingly Sophisticated Cyber Threat,” NEC Technical Journal, Vol. 9 No. 1, pp.123–127, 2015.1

Authors’ Profiles

YANO Yukiko
Senior Manager
National Security Solutions Division

ITO Atsushi
Manager
National Security Solutions Division

FUNAKOSHI Takeo
Manager
National Security Solutions Division

SATO Kazuyo
Manager
National Security Solutions Division

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Social trends & NEC's approach

Cybersecurity solutions

Applications of AI technology to cybersecurity

In-house efforts provide safety and security for customers

\Orchestrating a brighter world NEC
NEC Technical Journal
Cybersecurity
- Building Futureproof Security to Support Business Safety and Reliability -
Vol.12 No.2

Vol.12 No.2
January 2018

Special Issue TOP