2. Exercise: Incident Handling Procedure Testing

Main Objective	In this exercise participants will have the opportunity to learn the most important information about incident handling. It will give them an idea on how to organize this process in their teams in the most efficient way.	
Targeted Audience	This exercise is especially aimed at new CERT members. It can also be delivered to more experienced members to provide them with an opportunity to review their existing procedures and learn new methods of incident handling which will enable them to organize their work in a more efficient way.	
Total Duration	3 hours, 10 minutes	
Time Schedule	Introduction to the exercise	30 min.
	Task 1: Developing incident handling procedures	60 min
	Task 2: Resolving critical problems in incident handling	70 min.
	Summary of the exercise and evaluation	30 min.
Frequency	It is most important that this exercise be conducted with new CERT members or even with candidates. It could also be conducted periodically, to give more experienced team members the opportunity to evaluate and improve their existing procedures.	

2.1 GENERAL DESCRIPTION

The purpose of this exercise is:

- To familiarise participants with the basic set of activities relating to incident handling (IH) processes;
- To teach a correct sequence of activities during the IH process;
- To point out and provide knowledge about the most important parts of the IH procedure which critically influence the success of the process;
- To familiarise participants familiar all possible players in the IH process; and
- To provide participants with basic knowledge about the most effective methods of cooperation between CERT and key incident handling players.

2.2 EXERCISE COURSE

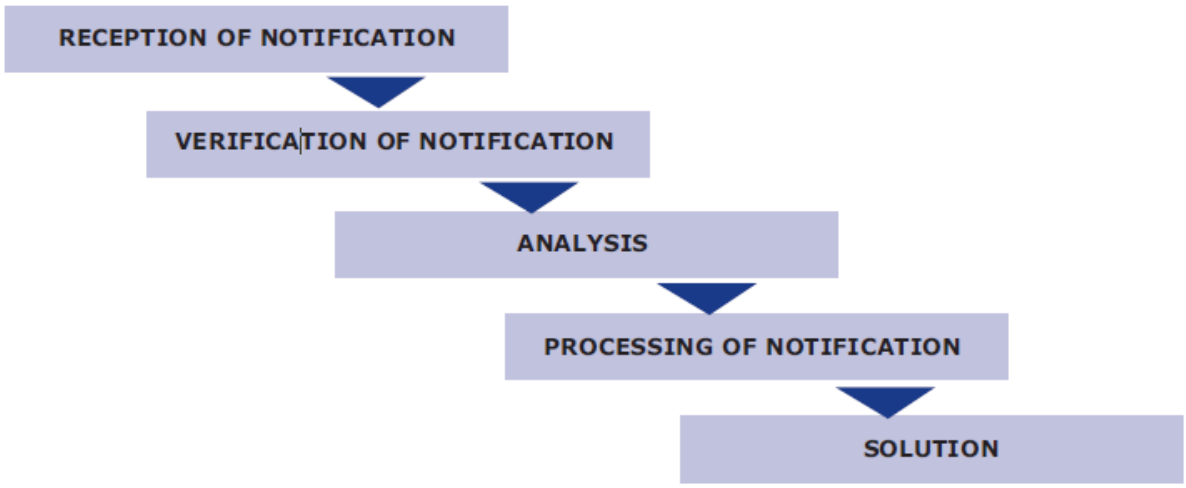
The course of this exercise is as follows. All discussions should be moderated by the trainer.

2.2.1 Introduction to the exercise

At the beginning of the exercise you present the students with some general information about the procedure for handling incidents. Define the most important part of the general procedure and explain the general sequences of a proper procedure. Also, at this stage, identify the most important players in the procedure.

To present a general concept of the incident handling procedure workflow you should describe the most important parts of it: reception of notification, verification of notification, analysis, processing of notification, and solution.

You can use the following schema:



Give students just a general overview of these phases. Do not explain in detail what kinds of activities are included in particular phases of the incident handling procedure, because this task will be part of the students' work. You should also mention incident handling procedure players, such as:

- 'Your' CERT,
- A reporter (an individual / an organization),
- A victim (an individual / an organization),
- An attacker (an individual / an organization),
- LEA (Law Enforcement Agencies),
- ISP (Internet Service Providers), and

- Other CERTs

When introducing these players, do not appoint a particular role for each of them as doing so will be a part of the students' work.

2.2.2 Task 1 Developing an incident handling procedure

After the initial, general presentation of the topic, continue with tasks for the students.

Divide the students into groups of 3-4 people. There should be at least two groups and preferably no more than four. Each group undertakes the following task:

Provide the students with the content of *Task 1.*

Using the objects of an incident handling procedure, form a complete incident handling procedure. Create the proper sequence of activities, build relations between them, and indicate the directions of the work flows. Additionally, extend the procedure with your proposals for activities using the blank objects.

After forming a procedure, identify activities which require communication with external parties. For each of them point out the recommended means of communication (eg, a normal email, a phone call, an encrypted e-mail, etc.).

Analyse your procedure. Specify the critical elements and identify the potential problems which could appear during execution of the procedures.

Use Appendix 1 for this task.

Give the students 30-45 minutes to complete this task. During that time, make sure you are available to answer any questions that may arise. Do not give hints and clues yourself – answer fully and correctly only when asked. After the time is up, give each group 5-10 minutes to present their procedure proposal. List all critical elements presented by each group on the whiteboard. During the presentation all students can ask questions. After the presentation they can ask questions or make comments, but they should avoid making a final evaluation of the procedures.

2.2.3 Task 2 Resolving critical problems in incident handling

After all procedures have been presented by the students, ask the whole group the following question:

Which procedure did you like the most and which one would you rather improve?

They must make a choice and explain their decision.

After they have had a discussion relating to their choices (about 30 minutes), ask the students to present their ideas on how to deal with the most critical parts of a procedure according to the list of problems identified by the groups during Task 1. Together with the students, create a list of the five most significant problems. This becomes Task 2 for the groups. You can form new groups for this task or you can keep the existing ones. Your decision can be influenced by the activity of the groups so far.

Provide the students with the content of *Task 2*:

Please write down the most critical parts of the procedure identified by the groups and the trainer. Provide your ideas on how to deal with them in order to mitigate related risks and propose proactive activities for avoiding such problems.

They have 20-30 minutes to discuss the problems within their groups and to present their solutions for mitigating these problems and the proactive actions needed to avoid them. After each group's presentation there is a short (5-10 minutes) discussion.

2.3 Summary of the exercise and evaluation

The whole exercise finishes with the summary made by you. Use the following schema to summarize the exercise:

- repetition of the main objectives of the exercise;
- description of the students' tasks and a short evaluation of their execution (see Evaluation Metrics for this exercise);
- description of the main parts of the incident handling procedure and the key players;
- enumeration of the means of communication in an incident handling procedure and a general description of the pros and cons of these means in terms of the efficiency and safety of the incident handling procedure; and
- summarisation of the problems identified by the students and the methods they would use to mitigate them.

The trainer should advise those students who already have their own incident handling procedure in their teams to self-evaluate the procedures.

2.4 EVALUATION METRICS

An intermediate method of evaluation could be a cross-evaluation by the teams of participants. During such an evaluation they would analyse the proposal for a procedure prepared by a different team and try to compare it to their own. They would try to point out the faults and good points of the proposal. In the end, the opinions are discussed and an arbitrary evaluation by the trainer is presented.

As more measurable factors in the evaluation, the following aspects could be checked:

- Have the students pointed out all key players in the incident handling process?

[Answer]

This is a relatively easy task as you mentioned these players in the introduction to the exercise. You should explain that most of the incident handling 'traffic' is exchanged between CERT teams. At this point you should also explain that the type and importance of a player is an important factor in incident handling prioritization. A special player is a LEA which is usually a

police department. It is important that your procedure corresponds to the law describing how the LEA must proceed.

- *'Your' CERT*
- *A reporter (an individual / an organization)*
- *A victim (an individual / an organization)*
- *An attacker (an individual / an organization)*
- *LEA (Law Enforcement Agencies)*
- *ISP (Internet Service Providers)*
- *Other CERTs*

▪ Have the students pointed all the key activities of the incident handling process?

[Answer]

The most important ones are:

- *proper determination as to whether a report constitutes an incident or not;*
- *identification of the real victim and the attacker in an incident, bearing in mind that the attacker identified in your report could be not the real one;*
- *activities related to alerting all interested parties about a threat related to your incident; and*
- *cooperation with the ISPs of the victim and the attacker for collecting and saving evidence of the incident.*

▪ Have the students enumerated correctly the most important means of communication and matched them to the relevant parts of the incident handling procedure?

[Answer]

The most important relationships and means of communication are:

- *CERT ↔ incident reporter*
  - *Email (do everything you can to ensure encrypted contact)*
  - *Telephone (ask a reporter to confirm a report by sending an email)*
  - *Web form (ensure encryption for this means (SSL))*
- *CERT ↔ LEA*
  - *Telephone (this means is mainly used by LEAs for obtaining initial information and consultation; use it widely as it is a very good educational 'system')*
  - *Official letter (this is an official document, so draft and deliver it according to the law in your country)*

- *CERT ↔ ISP*
    - *Email (the most common partners and means in the incident handling process, use the relationship actively, try to develop a trusted schema for getting a prompt answer, and use encryption for all confidential information)*

2.5 REFERENCES

To summarise the exercise, the trainer uses the references for graphical and descriptive information about incident handling procedure. He should also propose the following references:

1. ENISA, *A step-by-step approach on how to setup a CERT – Doing Incident Handling*, http://www.enisa.europa.eu/activities/cert/support/guide
2. Christopher Alberts (Carnegie Mellon University), Georgia Killcrece (Carnegie Mellon University), Robin Ruefle (Carnegie Mellon University), and Mark Zajicek (Carnegie Mellon University) - *Defining Incident Management Processes for CERTs: A Work in Progress* http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr015.pdf