CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE
DE SECURITATE CIBERNETICĂ – CERT-RO

ISACA

Incident Management

Author: Liliana Apetri

Incident Management is one of the critical processes in IT service management. It needs to be attended to on a continuous basis to better serve the company. Incident management focuses on providing increased continuity of service by reducing or removing the adverse effect of disturbances to IT services and covers almost all non-standard operations of IT services –thereby defining the scope to include any non-standard event.

Incident Management has the following steps:

- Incident report
- Registration
- Triage with the following steps: incident verification, incident initial classification, how to prioritize actions within your constituency, incident assignment.
- Incident resolution with the following steps: data analysis, resolution research, action proposed, action performed, eradication and recovery
- Incident closure: final information, final classification, archiving
- Post analysis: proposal for improvement
- Information disclosure
- Tools
- Quality assurance

1. Incident report

The most common way to report an incident is by e-mail. With appropriate systems the company may be able to detect incidents in the network and move them to the incident handling lifecycle. Below are a few methods for doing so:

- use the network monitoring systems (egg: intrusion detection systems or any other threat monitoring systems) to actively look for incidents in the network.
- monitor blacklists for records
- monitor forums and news websites for possible incident reports or threats.

2. Registration

Use of an incident report registration form could facilitate the registration process. If your company finds that an incident report is related to an already-registered incident it can decide to link or combine them together

3. Triage

The triage should determine the:

- significance of the constituency
- experience of the incident reporter
- severity of the incident
- time constraints

3.1 At the verification step, a report is examined as to whether or not it concerns a real incident.

3.2 Incident initial classification

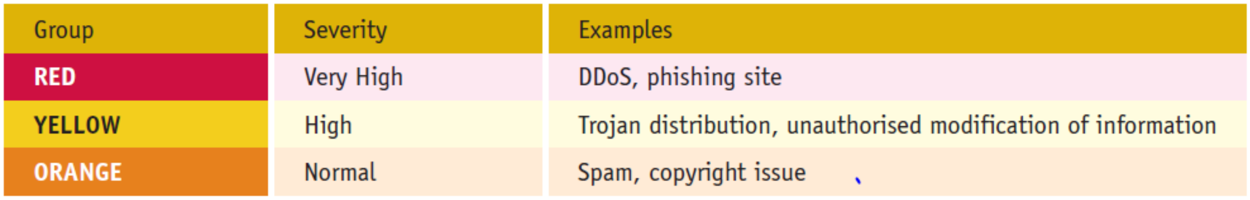
After verification, the company can initially classify an incident. It is classified according to the company classification schema. To decide how the incident is to be classified, the company try to determine as much information as possible from the report (and possibly other known reports).

3.3 How to prioritize actions within your constituency

Sooner or later the company probably will not be able to manage every incident at the highest level of effectiveness. It will be forced to differentiate the level of service. So the company will have to divide it's constituency into different categories according to your prioritization. While doing so it have to keep the company main tasks and mission in mind. If you are a company CERT then you are likely to be most responsive and provide services of the highest level for those company resources defined as critical. If you are a governmental CERT, your mission is to protect your country .gov domain, and if you are any other CERT with commercial contracts for an incident handling service, your goal is to deliver the best service to a paying customer.

Another factor to take into account in prioritization is the severity of an incident you are handling. The company could be dealing with a report about probing some computer in the network against well-known vulnerabilities and, at the same time, it could receive a report about a heavy DDoS attack. How do you manage it? Try to keep your prioritization mechanism simple.

Below table show basic prioritization of incidents by severity of attacks



Group	Severity	Examples
RED	Very High	DDoS, phishing site
YELLOW	High	Trojan distribution, unauthorised modification of information
ORANGE	Normal	Spam, copyright issue

Figure 1- Prioritization of incidents by severity of attacks

3.4 Incident assignment

Finally, in the triage phase, you assign an incident to an incident handler. There are many methods for doing that. You can simply decide that the handler is the person who first picked up the incident from the incident handling inbox. You can also have specialized handlers for particular types of incidents (egg: spam or malware), or finally you can have an incident handled by more than one handler according to their availability, specialization or other factors.

4. After the initial process of triage you start the incident resolution phase. This is the longest phase, which leads you to the resolution of the incident (or at least it should). You do it in the basic cycle: data analysis, resolution research, action proposed, action performed, and eradication and recovery

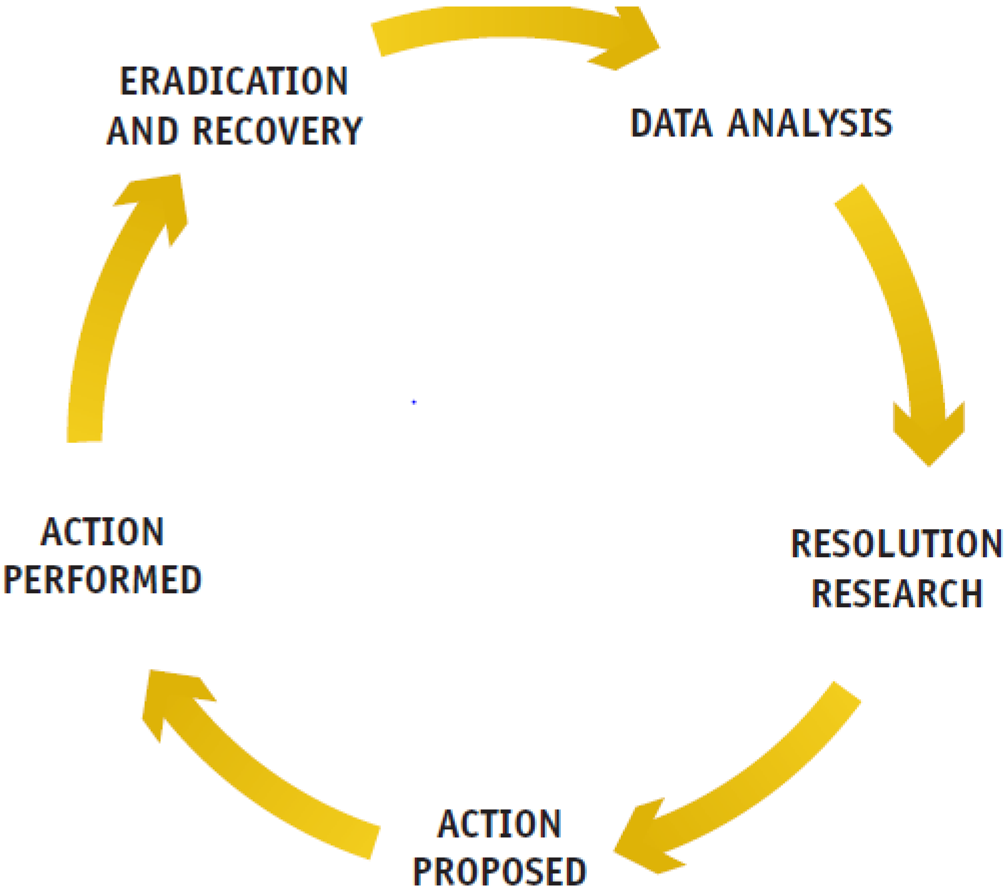


Figure 2 Incident resolution cycle

Usually one incident resolution cycle is not enough to solve a problem. Probably you will need to perform this cycle a few times in order to reach the desired result. There will be many times when you will not be satisfied with the final result, but some incidents are really difficult to handle and eradicate. Sometimes resolving an incident is simply outside your capabilities. If an incident is not critical in terms of its severity or the constituency it affects, this is not a very big problem.

Additionally, during the resolution of an incident, the situation can change significantly. For example, new attack targets can report new problems or an attack can become more sophisticated right after you thought you knew everything about it. Generally there is no other way to achieve success than to keep repeating the steps to resolve a problem.

4.1 First you inform those who may be the most affected. You may include in this notification some initial advice and information about further proceedings to resolve the incident. You should collect as much data as possible.

You have collected data and now you have to decide which data to analyze and in what order. To Decide on this, you can ask yourself the following questions:

- which data will most likely contain the information you need to resolve the incident?
- what sources of data do you trust the most?
- what security devices do you trust the most?
- what people do you trust the most?

4.2 Resolution research

To be successful in the resolution of an incident, it is not enough to know almost everything about an incident. Equally important is the timeliness of reaction. Sometimes a quick response has the same or a higher value than a comprehensive and complete set of information.

4.3 Action proposed

You have to be aware that in this phase of an incident, whether you want it or not, you are the incident owner. Most things depend on you. Therefore you should prepare a set of concrete and practical tasks for each party involved. Remember to adjust your language to your interlocutor. You can use quite advanced technical terms talking to another CERT or ISP, but you should switch to a 'descriptive mode' when giving advice to the attack target, unless you know (egg, from an incident report) that he is also a technically advanced person. Any action proposed should be clear and you should be sure that the recipient understands what you are proposing.

4.4 Action performed

There are some basic rules for monitoring the performance of actions:

Monitor technically whatever your are able to monitor, for example: Is the attack target's service turned off? Is the attack target's service still vulnerable? Is the traffic which should be filtered still visible in the network?

The execution of the rest of the actions can be checked by traditional means such as e-mail, phone or any other kind of direct contact. Use it to ask what has been done.

4.5 Eradication and recovery

The real resolution of a problem is to recover or restore to normal the service that was attacked during the incident. For example: it means that the application is working again, e-mails are reaching mailboxes, a website is available once more and displays proper content with proper response times, a computer is not part of a DDoS army and is not sending spam, etc. General speaking – an attacked system now does what it should do and not what it should not do.

5. Incident closure

You have left the incident resolution cycle. Now all you have to do is to close it properly. Below you can find the most important practices and advice on how to close an incident.

5.1 Final information

After resolving an incident you should inform the parties involved. There are two questions to answer. Who to inform and what to inform?

To answer the question ‘who’, consider contacting:

- a short description of the incident (including information about your classification of the incident);
- the results of your work – whether the incident was resolved or not;
- your main findings and recommendations

What should be included in the final information? Usually it does not make sense to bother contributors to the resolution of an incident with detailed information about the incident, especially if it is already well known and is merely being repeated. Adjust your information to the level of complexity of the incident. Generally you should consider attaching the following information to the final note:

- a short description of the incident (including information about your classification of the incident);
- the results of your work – whether the incident was resolved or not;
- your main findings and recommendations.

5.2 Final classification

If you pay attention to the classification of your incidents, you should analyze carefully when to finalize their classification. There are at least three points during the incident handling process when incidents can be classified. The first is at the start when you receive a report. At this point you can either do it yourself or use the opinion of the reporting party. The next point is during the resolution period when you learn much more about an incident and you are sure what it is exactly (whether you are right or not). And finally you can do it at the end of the incident handling process when you will know the most there is to know about it and what is most important, and when you probably will not be able to gain further useful information. Actually you can classify an incident three times, each time changing the classification.

5.3 Archiving

Generally there is nothing specifically different about archiving incidents in comparison to archiving any other data. It is worth remembering two important aspects:

- You probably will need to search your archived data quite often.
- Incident-related data is usually sensitive and you should apply appropriate security mechanisms to protect them.

In relation to searching an archived incident, the best option is if your main incident handling tools have the capability to archive data. Then you have direct access to them without any need to start a new application or go to additional resources. Usually in such a case, an incident handling tool has a search mechanisms built in as an application and the data can be searched while working on a particular incident.

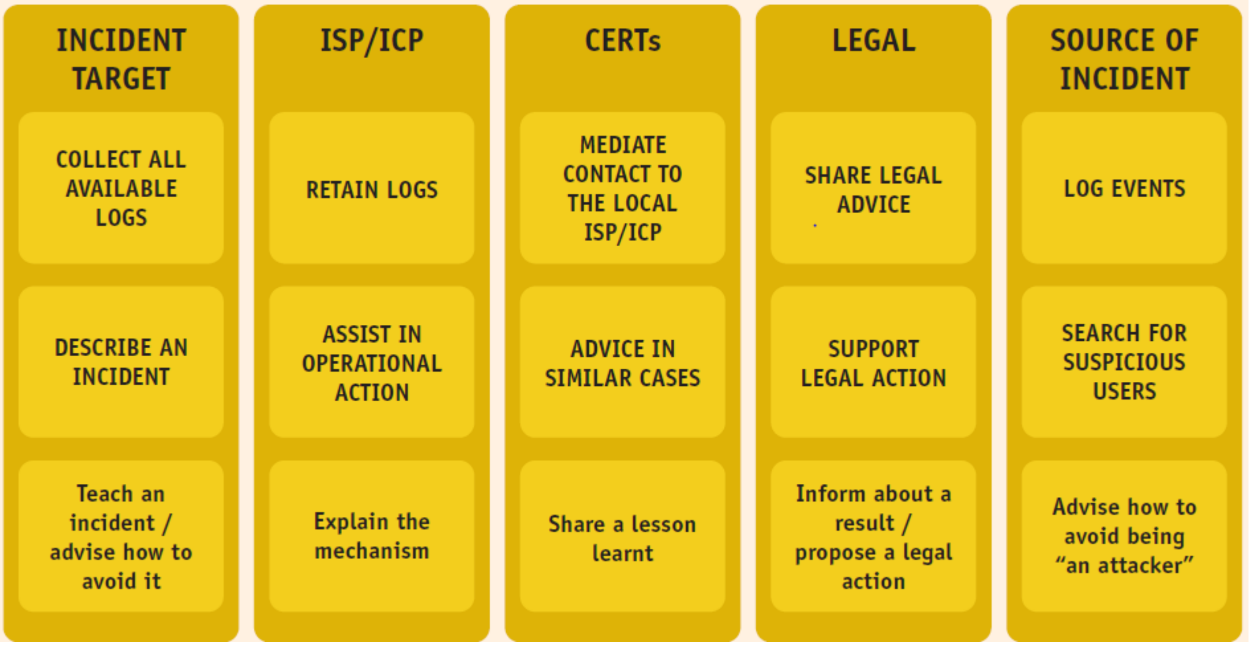
Remember that in most EU countries there are laws relating to data retention requirements and processing. Practically all these national laws are based on the EU Data Retention Directive. You have to follow the law related to this problem. After a period of legal data archiving, you must destroy that data.

6. Post analysis

Holding post-incident analysis sessions is a good idea for team self-learning sessions and for the exchange of information and ideas between team members. When organized periodically and systematically, they can be an important and valuable part of your team's professional life.

6.1 Proposals for improvement

Incident handling is, of course, a reactive service. It can be a first step to providing proactive actions for the improvement of security awareness. You can learn much from incidents you handled but you can also teach others a lot.



INCIDENT TARGET	ISP/ICP	CERTs	LEGAL	SOURCE OF INCIDENT
COLLECT ALL AVAILABLE LOGS	RETAIN LOGS	MEDIATE CONTACT TO THE LOCAL ISP/ICP	SHARE LEGAL ADVICE	LOG EVENTS
DESCRIBE AN INCIDENT	ASSIST IN OPERATIONAL ACTION	ADVICE IN SIMILAR CASES	SUPPORT LEGAL ACTION	SEARCH FOR SUSPICIOUS USERS
Teach an incident / advise how to avoid it	Explain the mechanism	Share a lesson learnt	Inform about a result / propose a legal action	Advise how to avoid being "an attacker"

Figure 3 Example of improvement proposals

7. Information disclosure

In your daily work it will be processing confidential information. You will receive such information from an incident reporter or other party participating in the incident handling process, for as long as you are considered a trusted organization. Introducing some simple but specific rules will help you to keep your 'trusted' status. So:

- Never disclose information that can specifically identify an attack target, unless you have his/her prior permission to do so. Even if you have permission – only do so if it helps resolve the incident.
- If you have to share sensitive information about an incident, make everything as anonymous as possible.
- Use encryption as a fundamental mechanism for data exchange and data archiving.

8. Tools

On the ENISA website these tools have been grouped into seven functional groups:

- gathering evidence from the scene of an incident
- investigating evidence of an incident
- supportive tools for handling evidence
- recovering the system after an incident
- implementing CSIRT operational procedures
- providing secure remote access
- proactive tools to audit or detect vulnerabilities and prevent incidents

9. Quality assurance

No matter how well you organize your incident handling process, how good are the chosen supporting tools and how good are the people who work in your CERT, you should always control the process. There is always something to improve, something to change and something to add to your actions.

Source: ENISA Good practice guide for incident management, CISA Review Manual 27 th Edition