Good Practice Guide for Incident Management

enisa
European Network and Information Security Agency

Table of Contents

MANAGEMENT SUMMARY

1 – Management Summary

This guide complements the existing set of ENISA guides[1] that support Computer Emergency Response Teams (CERTs, also known as CSIRTs). It describes good practices and provides practical information and guidelines for the management of network and information security incidents with an emphasis on incident handling.

This document implements one of the deliverables described in the ENISA Work Programme 2010[2], section 2.2.2.
The main focus area of the guide is the incident handling process – the core service carried out by most CERTs – which involves the detection and registration of incidents, followed by triage (classifying, prioritising and assigning incidents), incident resolution, closing and post-analysis.

Other topics covered by the guide include the formal framework for a CERT, roles (who does what), workflows, basic CERT policies, cooperation, outsourcing, and reporting to management.

For a CERT in the set-up stage this guide will provide very valuable input on how to actually shape incident management and especially the incident handling service. For existing CERTs, it can serve as a means to enhance their current services and to obtain input and ideas for improvement.

The primary target audiences of this guide are CERT technical staff and management.

1 ENISA's support for CERTs/CSIRTs: http://www.enisa.europa.eu/act/cert/support
2 ENISA Work Programme 2010: http://www.enisa.europa.eu/media/key-documents/enisa-work-programme-2010

2 – Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or any ENISA body unless it has been adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent the state-of the-art and it may be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources, including external web sites, referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

3 – Acknowledgements

ENISA wishes to thank all organisations and persons who contributed to this document. Particular thanks go to the following contributors:

- Miroslaw Maj MSc, Roeland Reijers and Don Stikvoort MSc(Hons) CTNLP, who created the first version of this document on behalf of ENISA
- the interviewed teams: CESNET-CERTS, CERT Polska, CERT-Hungary, CERT NIC.LV, and GOVCERT.NL
- the reviewers: Edwin Tump (GOVCERT.NL), Dr Klaus-Peter Kossakowski (DFN-CERT), Alan T Robinson BSc(Hons) MIET, and Pascal Steichen (CIRCL).

INTRODUCTION

4 – Introduction

4.1 Background

Communication networks and information systems have become an essential factor in economic and social development. Computing and networking are now utilities in the same way as electricity and water supplies.

Therefore the security of communication networks and information systems, and particularly their availability, is of increasing concern to society. This stems from the risks to key information systems, due to system complexity, accidents, mistakes and attacks on the physical infrastructures that deliver services. These services are critical to the well-being of EU citizens and to the functioning of governmental institutions, companies and other organisations throughout the EU and beyond.

On 10 March 2004, the European Network and Information Security Agency (ENISA) was established[3]. Its purpose is to ensure a high and effective level of network and information security within the Community and to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations within the European Union, thus contributing to the smooth functioning of the internal market.

Since 1993 a growing number of security communities in Europe such as CERT/CSIRTs, abuse teams and WARPs have collaborated for a more secure internet. ENISA supports these communities in their endeavours by providing information about measures for ensuring an appropriate level of service quality. ENISA also advises EU member states and EU bodies on matters relating to appropriate security services for specific groups of IT users.

Computer Emergency Response Teams (CERTs, also known as CSIRTs) are the key tool for critical information infrastructure protection (CIIP). Every single country that is connected to the internet must have the capability to effectively and efficiently respond to information security incidents. CERTs are able to do much more. They are in a position to act as important providers of security services to governments and citizens. At the same time, they have the opportunity to raise awareness of security issues and act as educators.

ENISA supports the establishment and operation of CERTs by publishing various reports on, for example, how to set up a CERT, how to run a CERT, CERT exercises, and more[4]. This document, the *ENISA Good Practice Guide for Incident Management*, is part of this series.

4.2 What this guide is about

This ENISA good practice guide provides a description of good practices for security *incident management*. The primary scope of incident management is IT and information security incidents, ie, incidents that are limited to computers, network appliances, networks and the information inside this equipment or in transit.

3 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency; a *European Community agency* is a body set up by the EU to carry out a very specific technical, scientific or management task within the 'Community domain' ('first pillar') of the EU.

4 See CERT section of ENISA webpage: http://www.enisa.europa.eu/act/cert/support

Throughout this document the term 'CERT' is used to describe any incident management capability, regardless of how it is labelled internally – as a team, service, process or function. The name 'CERT' (computer emergency response team) goes all the way back to 1989 and suggests an emphasis on 'emergency response', but this limitation does not exist today. CERTs not only react to incidents; they may also participate in the whole range of preventive measures (including awareness-raising), detection, resolution and 'lessons learnt'.

You may ask – why is effective incident management, why is a good CERT, so important? Why is it, in fact, essential for any organisation?

The answer is simple: when there is a fire, it must be extinguished. Anyone who has ever been in a fire wants to prevent it next time. It is the same with security incidents. Some time may pass without an incident – but they happen and will happen. Trend reports[5] show that incidents are not becoming fewer. On the contrary – they are becoming more advanced and targeted. Although some targets will be more popular than others, there are no safe hide-outs. For instance, even smaller schools in countries with languages spoken by small populations are being targeted these days. Banks, big networks, government and military entities are 'popular' targets. 'Hacktivism' has also emerged, where political or idealistic goals are used to justify what others would describe as cybercrime. Isolation does not help. Incidents can occur even if ample security measures are in place to shield an organisation from external threats via the internet. You should know that it has been reported that a substantial percentage of all incidents taking place has an internal source rather than an external one.[6]

You may ask – isn't incident management purely an IT issue? Can it be dealt with by capable computer people only? No, it is not just IT. Incidents threaten the organisation as a whole. The organisation's primary business process, all its other processes and reputation – they are all in jeopardy when incidents strike. Incident management seeks to prevent such incidents from happening. And when they do happen, to contain and resolve them, and use the lessons learnt for the next time. Therefore incident management serves the primary process and the organisation as a whole. The IT department may implement it, but it directly concerns the management of the organisation.

Thus, incident management is an important tool of overall governance and to have it, in whatever form or shape, is a necessity. This fact is recognised and supported in the ISO 27000 security standards[7] and in frameworks such as ITIL and COBIT.

This guide helps to provide a clear picture of the incident management process, so that its content, form and shape can be tailored to the specific needs of an organisation. The incident management process shows great variation in its implementation. For example, the 'resolution' process of a specific CERT can vary in scope all the way from being strictly limited to a coordinating and advisory role, to detailed hands-on solving of a specific problem in a specific computer. However the essence remains – prevent, detect and resolve incidents – and continuously learn from the process in order to improve outcomes.

Within incident management, this guide lays a special emphasis on incident handling. Incident handling is regarded as the quintessential incident management service – the core business of the majority of CERTs. Whereas specialised CERTs such as 'product security teams' will concentrate on, say, vulnerability handling, most CERTs actually handle security incidents.

5 See, eg, the GOVCERT.NL Trend Report 2009 : http://www.govcert.nl/download.html?f=152
6 More on inside threats can be found at http://www.cert.org/insider_threat/
7 notably so in the chapter on Information Security Incident Management' in ISO 27002

Incident handling has four major components (derived from CERT/CC[8] concepts), which are given here in the order in which incidents occur. First, an incident is reported or otherwise detected (*detection*). Then the incident is assessed, categorised, prioritised and is queued for action (*triage*). Next is research on the incident, what has happened, who is affected and so on (*analysis*). Finally, actions are taken to do all that is necessary to resolve the incident (*incident response*).

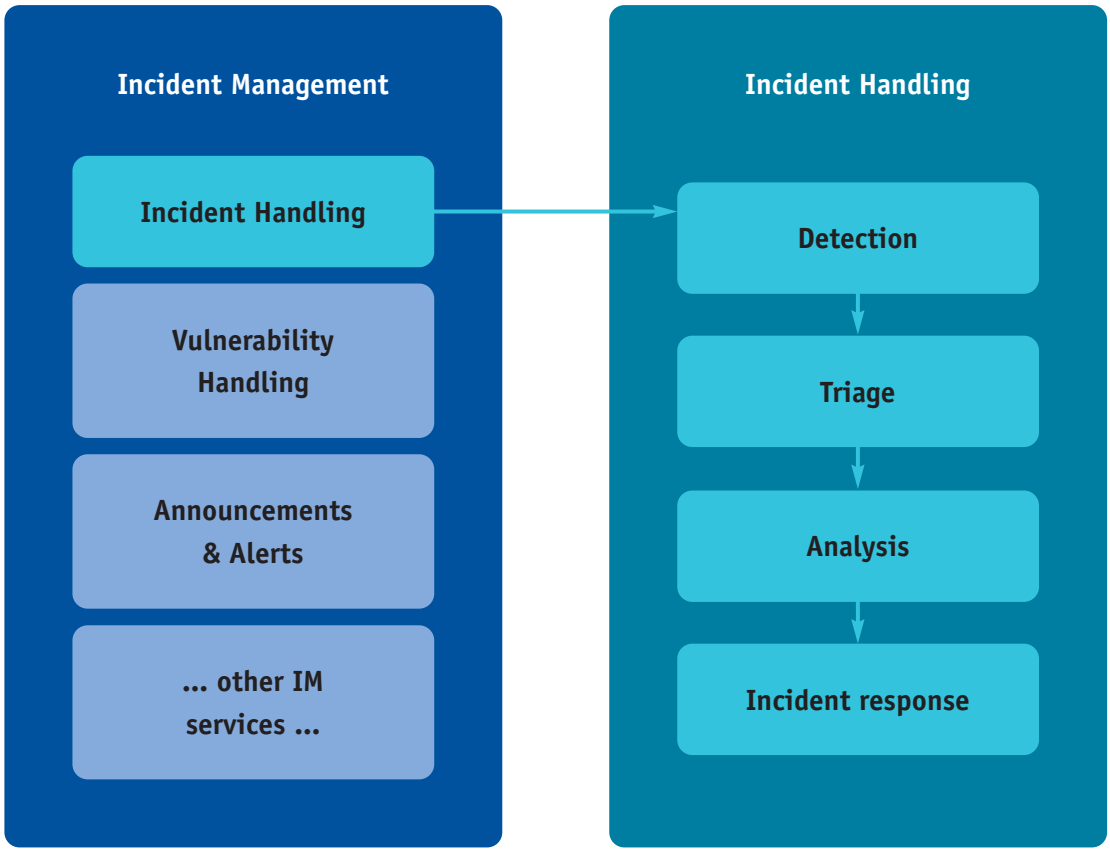


Figure 1 - Incident management and incident handling clarified

4.3 Target audience

The primary audiences for this guide are the technical staff and management of governmental and other institutions that operate (or will operate) a CERT in order to protect their own IT infrastructure or that of their stakeholders.

In general, any group or team that handles information or network security incidents, not just CERTs, but also abuse teams, WARPs and other security professionals, can benefit from reading this guide.

8 CERT® Coordination Center website: http://www.cert.org/

4.4 How to use this document

This document provides information on all aspects related to incident management, with an emphasis on incident handling. Starting from the basics of a CERT, its mission, constituency and authority, followed by the basic issues in incident management and handling, and finally all the way to, for example, outsourcing parts of your incident management service and making presentations to management.

Chapter 4 Introduction
This chapter provides the background and introduction to this guide.

Chapter 5 Framework
This chapter discusses the foundation of a CERT – its mission, constituency, responsibility, mandate, organisational framework – and the types of services the CERT can deliver.

Chapter 6 Roles
This chapter describes the roles that are mandatory and those that are optional in order to deliver a successful incident handling service.

Chapter 7 Workflows
This chapter describes the CERT/CC incident handling workflow and gives some examples of the workflows of other teams, how to use them in day-to-day operations, and how the incident lifecycle works.

Chapter 8 Incident Handling Process
This chapter describes the incident handling process in detail – from incident reporting via resolution to closing the incident. In addition, guidance is provided on information disclosure and relevant tools.

Chapter 9 Policies
This chapter refers to the basic policies a CERT needs to have in place in order to deliver its incident management service. In the second part of this chapter, the human resources aspect is highlighted.

Chapter 10 National and International Cooperation
This chapter discusses national and international cooperation. Various communities are highlighted.

Chapter 11 Outsourcing
This chapter provides an overview of outsourcing from the perspective of the CERT, focusing on the incident management service – what you could outsource or should not outsource, and how you can reach your goals while outsourcing.

Chapter 12 Presentations to management
This chapter is all about getting your management involved and keeping them involved – an essential factor in the success of your CERT.

Chapter 13 References
This chapter gives an overview of the most important documents on CERTs and incident management and how to use them.

Chapter 14 Annexes
Two annexes are provided: the first describes 'extended services', additional services that a CERT can deliver; the second annex is the 'CSIRT Code of Practice', a set of good behavioural rules.

Chapter 15 Figures Indexes
The figures index.

Chapter 16 Tables Indexes
The tables index.

4.5 Conventions used

The following conventions are used throughout this document:

- **Terminology CSIRT/CERT:** the term CERT (computer emergency response team) was used first in 1989 by what is now the CERT Coordination Center[9]. Their host organisation, Carnegie-Mellon University, registered 'CERT' as a trademark and service-mark in the USA. To avoid any trademark issues, the term CSIRT (computer security incident response team) was introduced a few years later by Kossakowski, Stikvoort and West-Brown in their CSIRT Handbook. CSIRT and CERT express the same concept – as does CSIHC (computer security incident handling capability) and IRT (incident response team). In this guide, the term CERT is used throughout to refer to an actual 'capability', ie, a service or function that provides for the management or handling of security incidents.
- **Gender specific language:** wherever in this document 'he' or 'his' is used, the reader is invited to also read 'she' or 'her'.
- **Logos:** the following logos are used:

where suggestions are being given to help the reader interpret and use the texts provided;

where 'good practices' are being described (also known as 'best practices' – a term avoided here as it is always debatable as to what constitutes 'best', with the answer usually depending on the circumstances);

where possible exercises are being suggested;

where reference is being made to tools;

where an example is being provided.

9 CERT® Coordination Center website: http://www.cert.org/

FRAMEWORK

5 – Framework

5.1 Mission

In the introduction you saw that incident management serves the organisation as a whole, not just IT. This means that to create a clear and useful mission for the CERT, you need to start with the mission of the organisation. If the organisation has a mission statement, description of its goals or charter, analyse it, discuss it and agree it with key people, including those responsible for the primary business process.

What is really essential for the organisation? It can be confidentiality, integrity, availability and/or other things. You need to find out how these can be impacted by incidents – use simple risk analysis for that. To minimise the chance that such incidents occur and to minimise the impact if they do occur is the goal of the CERT.

The mission of the CERT should therefore reflect what is really important for that specific organisation. Hence the mission statement of, for example, a CERT for a bank will differ from that for a biscuit factory or a government agency – though naturally the underlying idea of 'dealing with incidents' is a shared constant factor.

Apart from making sure that the CERT's mission reflects the organisation's mission, it is also a good idea to set a quality requirement within the statement, but not too tightly as usually a mission statement will not change for a couple of years. Be pragmatic – it is not realistic to say 'prevent any incident from happening', or 'resolve any incident within one hour'.

A better example of a quality requirement is this: 'the goal is to contain computer security incidents in such a way that their impact on the critical business processes is minimized'. This will give you a clearer benchmark to aim for and a standard against which to model your processes. It would, for instance, mean for an airline company with an internet booking system, that a 24/7 CERT is needed – because people will book flights at all times and this is an essential business process. If, on the other hand, the business process only runs from 9am to 5pm on working days, then it may not be vital to handle incidents in the middle of the night.

The mission statement should naturally also state what community the CERT cares for – towards whom their services are targeted. This is the so-called constituency.

5.2 Constituency: definition

For incident management you must define the constituency you work for or with – the *constituency* is the organisation (or group of organisations) and/or people whose incidents you handle (or co-ordinate). The question is: how best to define it? There are several different ways for defining constituency.
You can define your constituency by:

- range of IP addresses
- AS (autonomous system) number(s)
- domain name(s)
- free text description.

Some of these are specific to a particular company or type of organisation. Below you can find the types of definition of a constituency that are most often used and advised for particular types of institutions:

CONSTITUENCY DEFINITION TYPE / INSTITUTION TYPE	IP ADDRESS RANGE	AS NUMBER	DOMAIN NAME	FREE TEXT DESCRIPTION
FINANCIAL	●		●	●
GOVERNMENTAL	●		●	●
RESEARCH AND EDUCATION	●		●	●
INTERNET SERVICE PROVIDER	●	●		
VENDOR				●
INDUSTRY			●	●

Table 1 - Constituency definition preferences for different types of CERTs

5.2.1 Definition by range of IP addresses

In this type of definition you use the IP addresses which describe your constituency[10]. Usually you provide the range of IP addresses for your constituency. Examples of constituencies defined in this way are:

10 All the IP addresses presented in this chapter, as well as in the document as a whole, are publicly available (eg, FIRST.org website, Trusted Introducer website, CERTs websites, RIPE and similar databases). Please take into account that the affiliations of these addresses can change – this however does not affect the arguments presented here.

Team	Country	Constituency Definition
LITNET CERT	Lithuania	193.219.32.0/19 193.219.64.0/19 193.219.128.0/18 83.171.0.0/18
the ROYAL MAIL CSIRT	UK	144.87.x.x
University of Michigan CERT	USA	141.211.0.0/16 141.212.0.0/16 141.213.0.0/16 141.214.0.0/16 141.215.0.0/16 141.216.0.0/16

Table 2 - Examples of constituency definition by range of IP addresses

IP address ranges are present as *inetnum-objects* in the RIPE database in Europe, as RIPE is the European registry for IP numbers[11]. The RIPE database also allows you to register your CERT as an *IRT-object*. And subsequently, RIPE enables you and the registry of your IP addresses to refer to your *IRT-object* in the various *inetnum-objects*. This way, by looking at an IP address in the RIPE database, you can see immediately which CERT is responsible for handling complaints related to that IP address (see also section 8.9.1). In addition, reports about internet security issues can easily be routed to the appropriate team[12]! Note that if your team is accredited by the 'Trusted Introducer for CERTs in Europe' or TI[13], automatic generation of an *IRT-object* for your team is handled by the TI – but in such cases you still do need to work with your local IP registry to refer to that *IRT-object* from the *inetnum-objects*.

When you work with *IRT-objects* you will find that their popularity is gradually increasing – so many IP numbers are not yet linked to a CERT in this way. This is a shame, as the mechanism is available and simple to use – and there is no equal or better alternative. Wider usage would lead to better mapping.

Note that there is also the concept of an *abuse-mailbox* tag in the RIPE database, which is used to specify an e-mail address to which complaints about abuse or spam can be sent. The *abuse-mailbox* tag can be one of the lines in an *IRT object*, and thus give an additional e-mail address, the normal one for the CERT, and an extra one specifically for spam (these mail addresses can, of course, also be the same).

The *abuse-mailbox* can be found in other objects in the database as well, but remember that it is most definitely not a replacement for the *IRT object*, but only an addition to it (and to other objects). What a CERT does is much wider than just spam.

11 See RIPE NCC website: https://www.ripe.net. Similar registries exist in other regions of the world, such as ARIN for North-America.
12 If you decide to go this route, you can learn how to do so via the following link: http://www.ripe.net/db/support/security/irt/faq.html#q3
13 See Trusted Introducer's website https://www.trusted-introducer.org/ and section 10.6 Trusted Introducer in this guide.

5.2.2 Definition by AS number(s)

In this type of definition, you use the number of your AS (autonomous system) or multiple ASs if you have these. Examples of constituencies defined in this way are:

Team	Country	Constituency Definition
CERT NIC.LV	Latvia	AS5538, AS25444
KPN-CERT	The Netherlands	AS286, AS1134, AS1136, AS2043, AS3265, AS8737
TS-CSIRT	Sweden	AS544, AS1299, AS1729, AS1759, AS3301, AS3308, AS5473, AS5515, AS5518, AS5522, AS8233, AS8979, AS12582, AS12929

Table 3 - Examples of constituency definition by AS number(s)

As you may have expected, this type of description is typically used by the CERTs of internet service providers (ISPs).

5.2.3 Definition by domain name(s)

In this type of definition, you use a domain name in the form that describes your internet area of operation in the most accurate way. Examples of this type of description are:

Team	Country	Constituency Definition
ArCERT	Argentina	*.gov.ar; *.mil.ar
University of Michigan CERT	USA	umich.edu
dCERT	Germany	dcert.de, itsec-debis.de, debiszert.de, t-systems-dcert.de, t-systems-itc.com, t-systems-itc.de, t-systems-zert.com, t-systems-zert.de

Table 4 - Examples of constituency definition by domain name(s)

As you can see, there is no single standard for presenting the constituency by domain name. For example, you can use either '*.gov.ar' or 'dcert.de'. Both are acceptable.
It is also acceptable to describe the constituency in more than one way, eg, the University of Michigan CERT (see Tables 2 and 4 above) describes its constituency by range of IP addresses and by a domain name.

EXAMPLE

5.2.4 Definition by free text description

Very often the definition of a constituency is simply a description of whom the CERT cares for. You will see, for example, the names of companies or organisations or a description of the clients of organisations. Examples of such definitions are:

Team	Country	Constituency definition
ACOnet-CERT	Austria	Customers of ACOnet, Austrian Academic Computer Network
BadgIRT	USA	University of Wisconsin-Madison Faculty/Staff/Students
CERT Polska	Poland	All internet users in Poland
FSC-CERT	Germany	Customers of Fujitsu Technology Solutions
JANET CSIRT	UK	All UK organisations connected to JANET network
Cisco PSIRT	USA	Cisco Systems customers and products

Table 5 - Examples of constituency definition by free text description

This kind of description is quite clear but it is sometimes difficult to determine if a particular host address is or is not part of a particular constituency. And, as most incidents are attributed by means of IP addresses, this can cause ambiguity as to which CERT should deal with that incident.

5.3 Constituency: practical considerations

Note that every time there is a reference to the term 'constituency', this can be either an internal constituency, such as for the CERT of a company or organisation, or it can be any other type of constituency, such as a group of customers, government bodies or other organisations. Whether the CERT is mostly working inside an organisation, or is dealing with 'customers', or is a coordinating CERT or national team – the concepts remains the same. Whenever the discussion in this document is more specifically geared towards one of these categories, treat the matter as an example, generalise the ideas being expressed and apply them to your own specific situation.

5.3.1 How to establish contact with your constituency

As soon as you define your constituency you should establish active and good contacts within that constituency. Generally you can do this by means of a special announcement or by having regular meetings with your constituency if possible, but it is also worth supporting such a formal action by special or particular operational actions.

SUGGESTION

Below are some good ideas as to how you can quickly inform your constituency about your existence and, at the same time, convince them that you are going to work for their benefit and a more secure network:

- Inform constituency members about a particular threat with helpful advice on how to mitigate it.
- Inform constituency members of an attack on their infrastructure with instructions for attack mitigation and post-attack repair. A good occasion to do this could be during a massive attack on your constituency – eg, a determination that a large number of IP addresses are part of a botnet.

Remember that this is probably the best time to convince your constituency about your competence and usefulness. So be helpful and friendly, give something of yourself rather than expect to get something.

This first contact with your constituency is a very good time to give more information about who you are and what you are going to do. So inform your constituents about your services and mission. Try to do your best to avoid your message being treated as spam. It is better to refer to additional information than to put it in your message.

Regular meetings with your constituency can be very useful, as these are opportunities to present yourself, let your constituents share information on their ways of dealing with information security, share incidents, and let constituents or third-parties present solutions from which your constituents could benefit. It creates awareness, and sharing issues others have makes it easier for your constituents to talk about problems and ask for help if needed.

Also consider collecting information that will be useful for your team's operations. Practically any feedback will give you valuable information about your constituency, its expectations and how to contact them. Collect all this information, analyse it and make use of it – eg, by building a contact database and, where appropriate, adjusting your services to meet their expectations.

5.3.2 Overlapping constituencies

The constituencies of many CERTs overlap. This often happens when a constituency is described using a free description. For example, the constituencies of national CERTs are usually described as 'all sites in ...' or 'all Internet users in ...'. At the same time there can be many other CERTs in the same country so their constituencies must overlap. There is nothing really wrong about this. A description of a national level CERT should be treated as a declaration that it will handle incident reports related to its constituency (described as a whole country) rather than as a statement that it is the only organisation allowed to do so. Sometimes, when a CERT formally announces its claim over a part of another CERT's constituency, the latter team resigns from that part of its constituency and re-describes itself.

To avoid overlapping constituencies, analyse the constituencies of other CERTs in your country. If you do find overlaps – discuss them, negotiate and try to find a compromise.

5.4 Responsibility and mandate

5.4.1 Responsibility

The 'responsibility' of a CERT is what the CERT is expected to do according to its mission. It defines what the CERT must do in matters of incident management – and what its constituency and management can expect from it – including what they cannot expect.

A CERT's responsibility needs to be clearly described and then sanctioned by the highest management of the organisation for which the CERT works. This is necessary to make crystal clear to the constituency the matters for which the CERT is responsible when dealing with incidents for them and with them. Also, the management needs to know this – because it will hold the CERT accountable for delivering on its responsibilities.

When defining responsibility, the following practical questions should be taken into account:

- What types of incidents must be handled by the CERT, and with what priorities? This is essential as a new team, especially, can be swamped by wanting to handle all and everything. Making choices and setting priorities is a good idea right from the start.
- Must the CERT keep track of incident resolution and, at the end, close it? Or it is sufficient just to notify constituents to fulfil that task?
- Is the CERT obliged to actively solve an incident – which goes one step beyond guarding? Or just notify and give advice?
- Must the CERT escalate incidents when they do not get solved quickly enough and, if so, when and what must be escalated?
- Must the CERT inform specific entities about specific incidents? For example, when an employee may have done something 'wrong', must the CERT inform its management, or the management of the employee, or the human resources department?
- Think through the CERTs responsibility by examining specific incidents. Was the responsibility clear enough? Where can it be improved or extended?

5.4.2 Mandate

The 'mandate' of a CERT is the 'power' to do what it must do according to its mission. It defines what the CERT can do in matters of incident management – and what it cannot do.

The CERT mandate also needs to be clearly described and then sanctioned by the highest management of the organisation for which the CERT works. This is necessary to make the details of the mandate absolutely clear to the constituency. In addition, the management needs to know this so that, should the mandate of the CERT be ignored in some instance during a major incident, the CERT can bring the matter to the attention of management who will then know that they will need to act on this matter to avoid a deterioration in the situation.

When defining the mandate, the following practical questions should be considered:

- Does the CERT only give advice to its constituents, or can it also expect them to react in some way – such as giving acknowledgements, or even update reports – or can the CERT oblige them to solve the issue in a given time and keep the CERT informed? Of course the kind of reaction expected from a constituent may vary with the type of incident and its priority or importance – but the question remains, what and what not can the CERT expect from its constituents?
- Can the CERT give deadlines to its constituents to solve incidents? If they do not meet that deadline, what sanctions can the CERT impose? Can the CERT isolate them from the internet or corporate network, or impose protocol specific filters? Can the CERT escalate and to whom, just to its own management, or also to the constituent's management?
- Can the CERT just provide co-ordination and advice regarding an incident, or can it also actively gather data in constituents' computers, possibly do forensics, etc?
- Think through the CERT's mandate by examining specific incidents. Is the mandate well defined? Where can it be improved or clarified?

5.5 Organisational framework

5.5.1 Governance

The place of the CERT in the organisation and the governance model are of course discussed during the set-up phase. How to set-up a CERT is described in other ENISA guides[14]. However, some aspects of governance are essential to good incident management and need to be thoroughly considered and clearly defined. Those aspects are highlighted here.

5.5.1.1 Escalation

When an incident is serious and is not being solved quickly enough, and the CERT has exhausted the means within its own authority to handle and coordinate, the CERT must have a well-established and maintained mechanism for escalation. This escalation must reach an entity that, by its position and authority, can use other means to achieve a speedy solution to the incident in question, eg, by applying pressure to the constituent where the incident may apply.

This implies that escalation mechanisms can work in various ways.

The most usual form of escalation is to the higher management of your own organisation. Preferably this is the corporate or board level, and escalation then often leads to the CISO (chief information security officer) and/or CIO (chief information officer) first. The CISO/CIO informs the rest of the board – or the CERT does this directly in cases of emergency. The corporate level is the correct level to which a CERT should escalate, as this is the level from which the CERT derives its mission, its authority, its mandate and its responsibilities. Also, bear in mind that the CERT is not an IT department or an internal process of an IT department but, in fact, directly serves the primary process of the organisation as a whole.

Another option is an escalation to the senior management of a constituent, if that is where the incident is taking place.

An alternative combination of the above two mechanisms is used by the CERT of a major worldwide electronics company – here the CERT cannot, of course, 'stop production' when there are important incidents or threats, but it can issue 'yellow cards' and 'red cards'. Yellow cards are warnings that mean 'take this seriously, you need to act!'. Red cards actually go to the corporate level also and will lead to critical questions being asked at this level, the message being 'it is vital that you act quickly to solve this issue!'.

Whilst the CERT itself may be situated a few levels down in the organisation, it must have direct access to the highest level or a level just below that when escalation is necessary. An escalation model that follows the chain of command – step-by-step from low to high – will lead to unacceptable delays or misinterpretations when a grave incident occurs and is therefore not recommended in such cases. Of course, for incidents that are not grave and do not need urgent escalation, informing the next higher level of management is acceptable if this can help improve the issue. It is always a matter of prioritising, and thus severity and urgency can and should be used to decide what to escalate and to where. Common sense is needed here specifically as well – as always in security – because of the 'cry wolf' risk: you do not want to annoy your management with too many false alarms, because you will lose credibility that way. So do take enough time to think before you escalate.

---

14 See the ENISA document *Step-by-Step approach on how to setup a CSIRT* http://www.enisa.europa.eu/act/cert/support/guide and also section 13.1 How to use: *Step-by-Step approach on how to setup a CSIRT* in this guide.

5.5.1.2 Relationship with CISO and CIO (or equivalents)

As stated above, and it is something which applies universally, any CERT should establish and maintain a close working relationship with the CISO and/or the CIO of the organisation – or similar functions, such as the head of the IT department. Whoever it is, he or she must have a role with authority regarding security on an organisation-wide level and must also have access to the board or the CEO (chief executive officer). This is not only important for the escalation of incidents, but also for the prevention of incidents. The CISO and/or CIO play an essential role in security and thus in prevention; however the CERT is the one that deals with threats and incidents on a daily basis, so it has very good view of what can go wrong and when, and how to address it.

5.5.1.3 Relationship with crisis management in organisations

Many organisations have some form of crisis management. When very serious incidents occur, such as a fire or negative media attention with a risk to credibility and reputation, the crisis manager assembles a team whose only task becomes tackling the crisis until it is solved and the team can be disbanded again. Such teams are typically a mix of governance level executives (to take decisions and to gauge the business impact), case experts (to understand what is happening and what needs to be done), public relations (PR) officers (to explain what is being done) and legal counsel (to understand what can be done and must be done, and with what legal consequences).

Serious incidents these days very often will have an important IT dimension, and involve security incidents, real or potential. A fire is an obvious example as it will disable or destroy computers and networks with the potential to create negative feedback from the public (eg, press, internet blogs). Every leaked e-mail with partial or wrong information could worsen the situation. This is the domain of the CERT. Therefore the CERT should establish and maintain a close working relationship with crisis management in the organisation. Where appropriate a CERT member can be part of a crisis team.

In addition, IT security incidents can be so grave that they themselves lead to the formation of a crisis team. In that case the CERT needs to directly address the crisis manager.

In cases where CERTs have constituents outside their organisations, such as, for example, branch or commercial CERTs, their local contacts within their constituent's organisations need to have close relationships with their crisis management. In the case of a national CERT, a good working relationship with a national crisis and coordination centre is needed for when national crises arise.

5.5.2 Human Resources

Fulltime or part-time human resource models are most common among CERTs. Yet there are other possible models which may be adopted to manage possible shortages of personnel. Exchange programmes, student internship programmes, volunteering, and outsourcing are discussed here.

5.5.2.1 Fulltime and part-time

A dominant model is regular full-time employment, particularly nowadays as there are more and more CERT teams around the world and they play a significant role in the security structures of their countries and constituencies. The part-time employment model is usually used when team members have more than only CERT-oriented obligations. For example, they are network administrators or members of an organisation's security team. Very often this model is encountered when there is no regular CERT in the organisational structure and the team is a virtual one.

The virtual team can operate very smoothly. The only problem is that the team members have other daily responsibilities and they have very limited chances to provide more incident management related services other than incident handling. Such solutions however are used quite often in situations when the incident handling capability is required by corporate policy or law. Anytime you feel you should or wish to do more and launch new services is probably the best time to reorganise the virtual team and to form a regular CERT team. Members of a virtual team are natural candidates for this newly established 'real' team.

If you decide to have part-time CERT employees, you should ensure that you are not sacrificing the continuity of the incident handling process. Of course, other CERT services are also important but this is the core activity. As your part-time team members are unlikely to deal with CERT work on a daily basis, the practical advice is to determine critical situations and ensure that when these occur appropriate staff can be notified. The remaining tasks can be done during the regular part-time work.

5.5.2.2 Exchange programmes

The exchange programme is not a common example of cooperation between CERT teams. However, those who have opted for it hold it in high regard. Working together with people from different teams is a great experience and it provides a lot of benefits to both sides, especially:

- sharing experiences from incident management work;
- learning about incident management procedures used by other teams;
- establishing closer personnel cooperation;
- learning about new incident management tools;
- learning about cooperation with a team's constituency.

When considering this option you should keep in mind some of the potential problems related to this kind of cooperation, such as:

- communication problems in studying incident management activities (eg, language barriers);
- employment rules for longer exchange periods;
- strict disclosure policies in some teams (eg, governmental teams). Such policies can limit or exclude the possibility of sharing incident related information.

SUGGESTION

If you wish to implement an exchange programme, Figure 2 below presents a proposal for a four-week exchange programme.

CERT EXCHANGE PROGRAMME

WEEK 1

- ASSESS INCIDENT MANAGEMENT PROCEDURES
  - present your own procedures
- ASSIST IN INCIDENT MANAGEMENT
- ASSESS CONSTITUENCY
  - find differences between the constituencies

WEEK 2

- ASSESS INCIDENT MANAGEMENT TOOLS
  - propose new tools (from your toolkit)
- ASSESS COOPERATION WITH OTHERS (eg, ISP, LEA)

WEEK 3

- DEVELOP IDEAS FOR COMMON INCIDENT
- MANAGEMENT PROCESSES
  - Incident management procedures
  - Incident management tools
  - cooperation with constituency, ISPs, LEAs
- IMPLEMENT CHOSEN AND ACCEPTED IDEAS

WEEK 4

- WRITE 'LESSONS LEARNT' REPORT
  - what is good in the other team's operations?
  - what could be improved in your opinion?
  - what could be exchanged between the teams?
  - what could be shared by the teams?

Figure 2 - Idea for a CERT exchange programme

5.5.2.3 Student internship

A student internship programme is yet another possibility for enriching the CERT. It is also a good way to find potential new employees for your team. Interestingly, not only students in network or network security fields can practice in your team; you can get benefits from students from other disciplines as well.

EXAMPLE

The table 6 presents some examples of fields of study and potential topics for a student internship programme (in terms of benefits for the incident management process).

FIELD OF STUDY	STUDENT INTERNSHIP PROGRAMME TOPIC
Economics	Cost of incidents
Philology (various)	Monitoring of different language internet fora
Geography	Geographical distribution of security incident related data (eg, using GIS (geographical information systems))
Informatics (software development)	Development of incident management supporting tools
Sociology	Monitoring and doing research on underground internet criminal groups

Table 6 - Ideas for student internship programme topics

It is important that the student internship programme will benefit both sides. Students will learn from your work and will find potential topics for their further education. You improve your work and your incident management process. The best way to achieve this is to prepare properly for the internship. Discuss with the student volunteers their interests and motivations and how they will use the opportunity to develop their skills and contribute to the team. Try to be active in developing ideas for the internship and finally be helpful, but also demanding, during the internship. Remember that only when you are able to put effort into the students will you back get the results that can help you.

5.5.2.4 Outsourcing[15]

Another way of implementing incident management is to outsource part of it. As incident management activities are potentially very sensitive, such a decision should be considered very carefully and requires continuous monitoring. You can outsource your whole incident management service (but then in practical terms you are not a CERT anymore) or part of your overall process. So the only recommended model is to outsource only a part of the whole incident management process. For more detail on outsourcing, see chapter 11 Outsourcing.

5.5.3 Central versus distributed model of operation

Some CERTs work from a single location. Others have distributed locations; for instance, some team members may work for a particular part of an overall constituency, eg, by being a member of some organisation other than the parent organisation of the CERT. Incident handlers in many organisations working together could create the distributed model of a CERT. This model can be seen quite often in the academic sector where many network administrators report any security problems to one central place.

Another case in which the distributed model works is in the CERT of a company with a lot of branches (eg, international ones). Within the branches, people report and coordinate security incidents with a central CERT located at company headquarters[16].

15 For more details about outsourcing, go to the chapter 11 Outsourcing.
16 See the TS-CERT (Telia Sonera CERT) which operates in seven countries: Denmark, Estonia, Finland, Latvia, Lithuania, Norway, and Sweden: http://www.first.org/members/teams/ts-cert/

How is this relevant to incident management? Mostly in three ways:

- A CERT is the hub of the incident handling wheel. However, actual incidents usually occur at the perimeter of the wheel, where the constituents are. In most cases the CERT has to rely on the constituents to actually resolve the incidents. A distributed CERT can be a great advantage there, as it allows CERT people to be where they are most needed – close to where incidents happen. They know the local systems and the local people, and can thus help to solve an incident faster and more efficiently.
- A geographically distributed CERT, with offices dispersed over multiple time zones, could be useful in creating a round-the-clock CERT.
- A distributed approach can have a negative effect on incident handling due to the more complex organisation and associated logistics of a distributed CERT compared with a centralised CERT. So when a choice is made to have a distributed CERT, it must be organised well, particularly regarding communications, IT, logging, access to CERT systems, hand-over of duties, team meetings, etc.

5.6 Service types

The traditional catalogue of CERT services is presented in the table (Table 7) of CERT services developed by the CERT Coordination Centre.

CERT SERVICES		
REACTIVE SERVICES	**PROACTIVE SERVICES**	**SECURITY QUALITY MANAGEMENT SERVICES**
● ALERTS AND WARNINGS	● ANNOUNCEMENTS	● RISK ANALYSIS
● INCIDENT HANDLING	● TECHNOLOGY WATCH	● BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING
● VULNERABILITY HANDLING	● SECURITY AUDITS OR ASSESSMENTS	● SECURITY CONSULTING
● ARTIFACT HANDLING	● CONFIGURATION AND MAINTENANCE OF SECURITY TOOLS, APPLICATIONS AND INFRASTRUCTURE	● AWARENESS BUILDING
	● DEVELOPMENT OF SECURITY TOOLS	● EDUCATION TRAINING
	● INTRUSION DETECTION SERVICES	● PRODUCT EVALUATION OR CERTIFICATION
	● SECURITY-RELATED INFORMATION DISSEMINATION	

Table 7 - CERT services in terms of the incident management process

As you can see in the table above there are three main types of CERT services. You can use this list for making a decision about the set of incident management services you offer initially.

Services marked in red are closely related to the incident management process. The absolutely essential minimum in the context of a CERT is the incident handling service, which is the focus of this guide. For more information on other services see 14.1 Annex I – CERT extended services in this document and Appendix A.2 in our guide *Step-by-step approach on how to set up a CSIRT*[17].

17 *A step-by-step approach on how to set up a CSIRT*: http://www.enisa.europa.eu/act/cert/support/guide

ROLES

6 – Roles

For incident management to be successful, it is essential to carefully consider the roles within a CERT and to tailor these to your specific mission, constituency and environment.

A CERT can be a virtual team with no formal members and with tasks distributed between different employees in various company departments such as the network operations centre, internal IT security team, legal department, PR department, help desk, etc. It can also be a department in a company's organisational structure, with several core members but also with some members from different departments, who work part-time or only on a specific task. Finally it can be an organisation or department with only full-time members. The information you will find below is useful in any of the types of organisation structures mentioned previously. The roles described here have been selected while keeping the core CERT service – incident handling – in mind.

The roles can be divided into mandatory roles and optional roles.

6.1 Mandatory roles

The mandatory roles are:

- Duty officer

A duty officer has to take care of all in-coming requests as well as carry out periodic or ad hoc activities dedicated to this role.

- Triage officer

The triage officer has to deal with all incidents that are reported to or by the team. He needs to decide whether it is an incident that is to be handled by the team, when to handle it and who is going to be the incident handler according to the triage process[18].

He needs to be up to date with all the latest trends, attack vectors and methods used by miscreants. In many cases the duty officers are also the triage officers.

- Incident handler

The incident handler is a crucial role in the incident handling team. He deals with the incidents – analysing data, creating workarounds, resolving the incident and communicating clearly about the progress he has made to his incident manager and to and with the appropriate constituent(s).

- Incident manager

The incident manager is responsible for the coordination of all incident handling activities. He represents the incident handling team outside his team.

This mandatory role can be fulfilled either by a dedicated person without incident handling obligations, or one of the more senior incident handlers. It is important that this person has a technical background and experience and that he understands current IT security threats. One possible solution is to rotate the role of incident manager around a number of suitable individuals.

18 See section 8.3 Triage

It is important to continuously monitor the workload of the team, particularly incident handlers. If you have more and more incidents you can:

- increase the number of incident handlers;
- decrease the level of involvement in incident resolution;
- develop techniques for automation in incident handling[19].

If only limited resources are available, all the roles mentioned above can be performed by just one or two persons. This is very rare and is not recommended.

In the table below you can find information about daily tasks, periodic tasks, position in organisational structure and competence[20] for all of the mandatory roles.

POSITION	DAILY TASKS	PERIODIC TASKS	POSITION IN ORGANISATION	COMPETENCE
DUTY OFFICER	Ensure that all incidents have owners Be available during service hours	Hand over all remaining work and 'state of the world' to the next duty officer at the end of duty	Junior staff	Basic technical knowledge Communication skills Accuracy Analytical skills Stress resistant
TRIAGE OFFICER	Check for new incidents Triage incidents in terms of their legitimacy, correctness, constituency origin, severity[21] (constituency/ impact) Hand over incidents to incident handlers in cooperation with the incident manager Report problems with incident overload	Discuss new kinds of incidents, trends with team members	Junior staff	Knowledge about existing threats Communication skills Accuracy Analytical skills Stress resistant

19 To learn more on how to do this, check exercise 10 – 'Automation in Incident Handling' from the ENISA *CERT Exercises Handbook* http://www.enisa.europa.eu/act/cert/support/exercise/

20 To learn how to check competence and how to recruit for your team, you can use exercise 3 – 'Recruitment of CERT Staff' from the ENISA CERT Exercises Handbook http://www.enisa.europa.eu/act/cert/support/exercise/

21 For detailed tasks, see section 8.3 Triage.

POSITION	DAILY TASKS	PERIODIC TASKS	POSITION IN ORGANISATION	COMPETENCE
INCIDENT HANDLER	Analyse incidents assigned to him Resolve incidents[22] Fulfil tasks of a duty officer or triage officer if needed Escalate if necessary	Propose improvements in incident handling process Acquire knowledge about new types of incidents	Junior or senior staff	Advanced IT security technical knowledge Strong communication skills Strong analytical skills Able to cooperate Stress resistant
INCIDENT MANAGER	Coordinate day-to-day work of incident handling team; decide how to act in problematic situations Check fulfilment of daily tasks Represent team within the CERT, within the organisation and outside the organisation Advise on how to handle incidents Escalate if necessary	Propose improvements for incident handling team work Discuss balance of incident assignments with incident handlers and triage officers Organise periodic meetings for discussions about incident handling work within team Report to higher management, CISO/CIO, etc	Senior/ management staff	Advanced IT security technical knowledge Communication and PR skills Strong analytical skills Management skills Stress resistant

Table 8 - CERT staff roles, tasks, positions and competencies

6.2 Optional roles

The following roles are optional, but in many cases part or all of the tasks that would fit the roles have to be undertaken in some way. These tasks do not necessarily have to be carried out by the incident handling team, but can also be undertaken by people in the hosting organisation.

- Public relations officer
- Legal officer
- Team manager
- Hotline operator.

22 For detailed tasks, see section 8.4 Incident resolution.

6.2.1 Public relations officer

The main task for the public relations (PR) officer is to represent the team in front of the press and give advice to team members in any situation that could have PR consequences. The PR officer is especially important if you are a governmental or national CERT or a CERT representing a company with a high media profile. If you do not or cannot have a PR officer within your team, use company resources and assign this role to the incident or team manager. Always keep your PR officer well informed, but be cautious and clearly communicate which part of the information shared is for internal use only, so that it does not get disclosed accidentally.

One of the most important tasks for a PR officer is to develop a crisis communication strategy. You have to be prepared for the worst in case an incident leads to difficult questions about your response or the impact on your constituents. A PR officer should also provide media training for your team members.

You will find examples of good practice in an interview with Kelly Kimberland – PR manager at CERT/CC[23].

More on media policies can be found in section 9.1.3 Media policy.

6.2.2 Legal officer

The legal officer ideally takes care of special situations arising from incidents and the team's internal processes in terms of their compliance with the law. Your legal officer can be of great help to you, as he or she knows the law, your liability and your contracts. Of course it helps when the legal officer has an understanding of the specific legal aspects of IT matters.

A legal officer generally operates in two situations:

- when your team needs advice on specific legal issues regarding incident management, which can for instance influence the way that operations are done or presented, evidence is collected, data is verified and retained, and so on;
- when a constituent or other stakeholder asks your CERT for legal advice.

The first case is standard and is essential in your work. If you do not have a designated legal officer you should use external resources to learn the basic rules for your daily operations.

It is good practice to train one or a few team members in the most important legal aspects related to your activities. In any group you can usually find one person who is interested in law.

Sometimes it is useful to be aware of the law not only in your own country but also in countries where there are teams with whom you coordinate and resolve incidents. *The Handbook of Legal Procedures of Computer and Network Misuse in EU Countries*[24] will provide you with help about other legal systems in the EU.

23 'Crisis Communication During a Security Incident' (podcast transcription) – http://www.cert.org/podcast/transcripts/13kimberland.pdf/
24 *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries*: http://www.rand.org/pubs/technical_reports/TR337/

6.2.3 Team manager

If your CERT team is bigger than just the incident handling team, there is a need for a CERT or team manager. For example, in a CERT where you have an incident handling team, R&D team, forensic analysis team, malware analysis team, and an awareness team, having a team manager is really necessary. The tasks of a team manager are to coordinate team activities, balance workload, and provide a strategy – in short, manage the team. When dealing with many incidents or major incidents, the team manager is also a point of escalation for the incident manager.

In the situation where the CERT is just a small organisation, it may not be possible for you to have a dedicated team manager position. In such cases, probably the best solution is to nominate the incident manager to act as the team manager. The incident handling service is the core CERT service and this person is the one who is most aware of the issues that need to be resolved and prioritised so work can be coordinated. Be aware, though, that managing incidents can be a challenging task. Time may not be available to also manage other parts of the organisation.

6.2.4 Hotline operator

If you have many requests, inquiries or general calls other than incident reports, you could appoint someone as a hotline operator. The main task of the hotline operator is to promptly react to all standard requests and forward these requests to other team members as needed. Normally the duty officer would handle this role.

The tasks related to this role include call handling, providing basic responses and answers to enquiries, and forwarding requests to the appropriate persons.

WORKFLOWS

7 – Workflows

7.1 Proposed workflows

You can find the most fundamental description of the incident handling workflow in the CERT/CC document referenced below[25]. It has four main phases:

- detection
- triage
- analysis
- incident response.

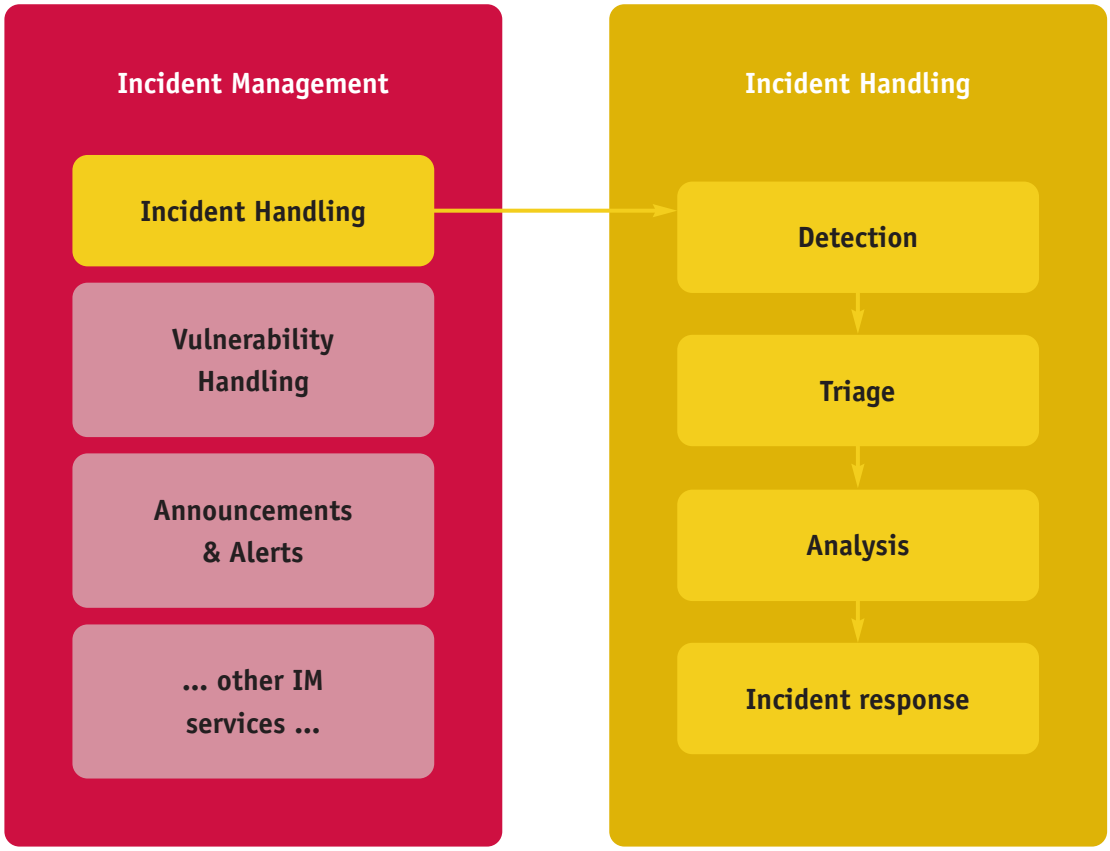


Figure 3 - Incident management and incident handling

You can extend this approach and add more detail. For example, you can find another basic and more extended model workflow for incident handling in the ENISA document – *Step-by-step Approach on how to set up a CSIRT*[26].

25 *Defining Incident Management Processes for CSIRTs: A Work in Progress* – http://www.cert.org/archive/pdf/04tr015.pdf
26 *ENISA CSIRT Setting-up Guide*: http://www.enisa.europa.eu/act/cert/support/guide

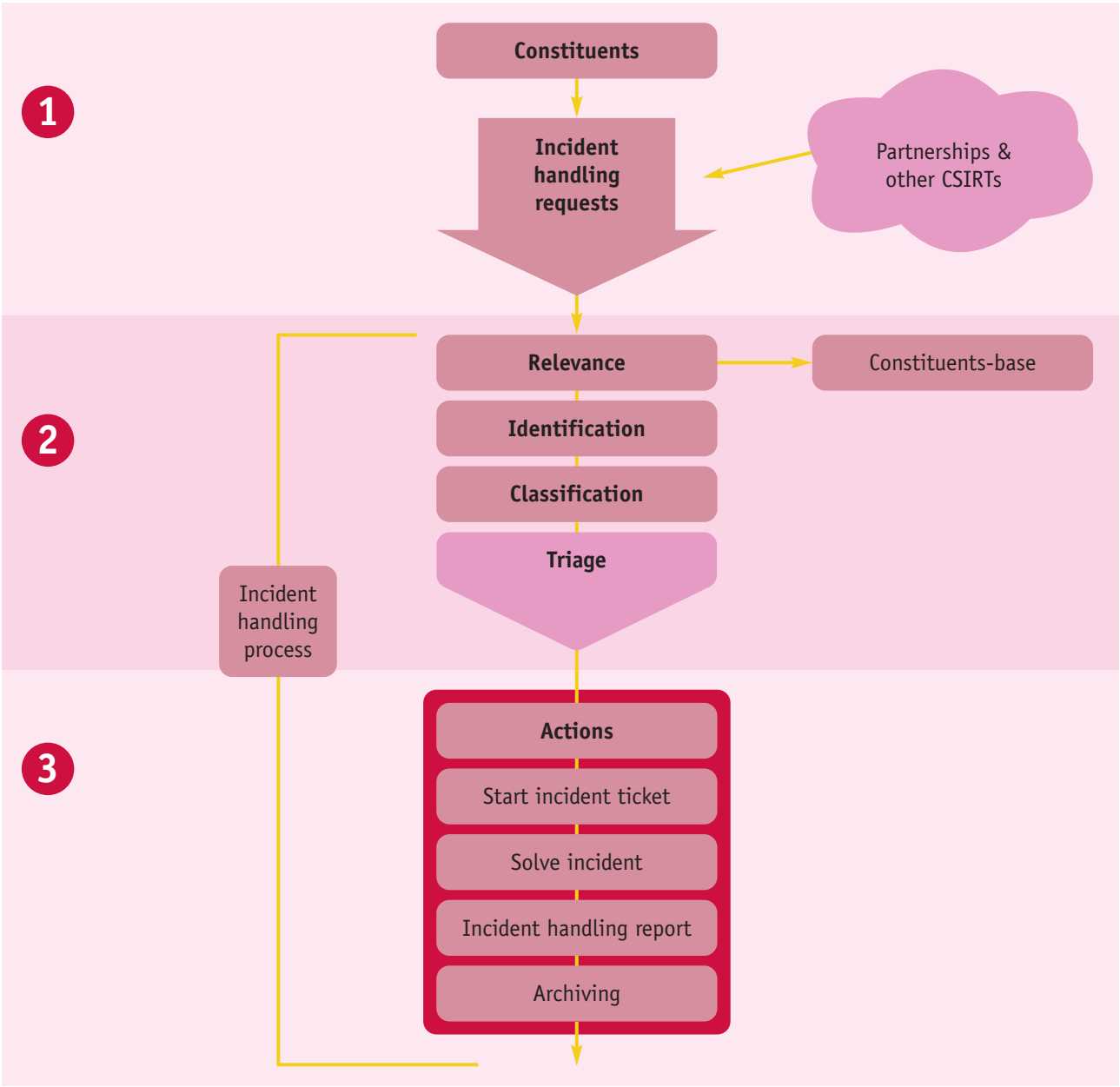


Figure 4 – Incident handling process flow

Figure 4 gives a general overview of each phase of the incident handling process. Before you decide on your detailed workflow, it is worth examining other examples of models and use them to develop your ideas, expectations and vision for your future model. Keep in mind that this workflow is close to your day-to-day operations and the workflow should enable your team to do the work more efficiently and not hinder the work. Below you can find some further examples.

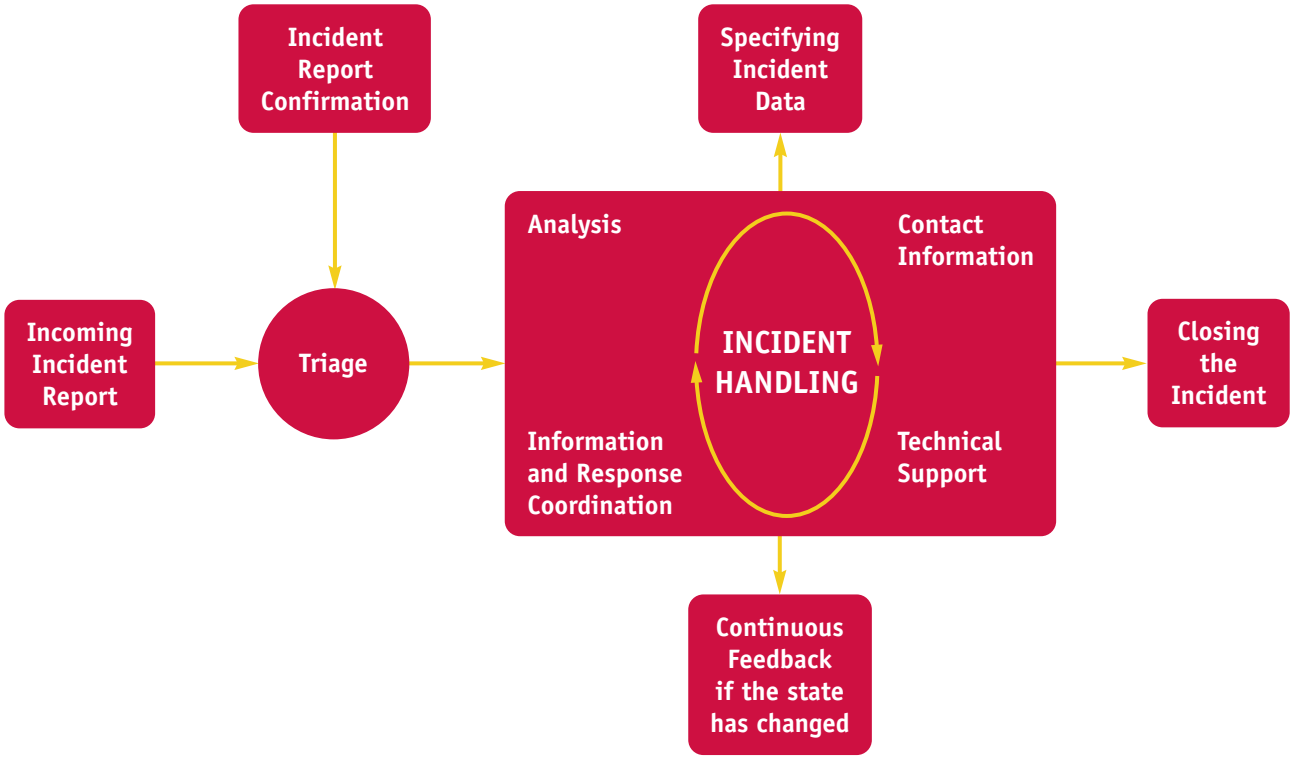


Figure 5 - Incident handling process flow (CERT Hungary example)

Figure 5 represents the workflow used by CERT-Hungary – again derived from CERT/CC concepts. As you can see, everything starts with an *incoming incident report* followed by the triage process, which includes *incident report confirmation*. After this, the core part of the process (incident handling) starts. It consists of four phases in one cycle:

- analysis
- contact information
- technical support
- information and response coordination.

Very important parts of this cycle are the continuous activities of *specifying incident data* and *feedback* between incident handling parties *if the state has changed*. All activities mentioned should lead to *closing the incident*. Therefore, as you can see, it is possible to extend the workflow and include other or more steps. Every step can be detailed with specific checklists.

An example could be a checklist for the duty officer or triage officer. The following questions should be part of such a checklist:

- Check if a report includes a full e-mail header?
- Check if an incident relates to your constituency?
- Check if there is a trusted CERT team for the constituency from which you are going to collect data?
- Check if you had a similar incident in the past (for consistent incident classification)?

If, over time, the workflow and checklists become too detailed, the key question you need to ask is: is such a workflow and checklist practical for the daily work of your team? In many cases it is not practical. The incident handling process is quite intuitive and you do not need such a complex approach.

This does not mean it is completely worthless to develop these workflows and checklists. Developing them is a very educational process. The involvement of all your team members in this development can produce a common understanding of how your team works. It is very useful for self-learning on how to deal effectively with incidents.

It is good practice to organise periodic (eg, twice a year) workshops to develop and review a common incident handling workflow. During such meetings, team members can propose very detailed parts to the workflow.

To assist you in reaching this goal, you can also use Exercise 2 – Incident Handling Procedure Testing, in the ENISA CERT exercises materials[27].

A good approach to this problem is to prepare a general workflow that includes all the most important phases of the process.

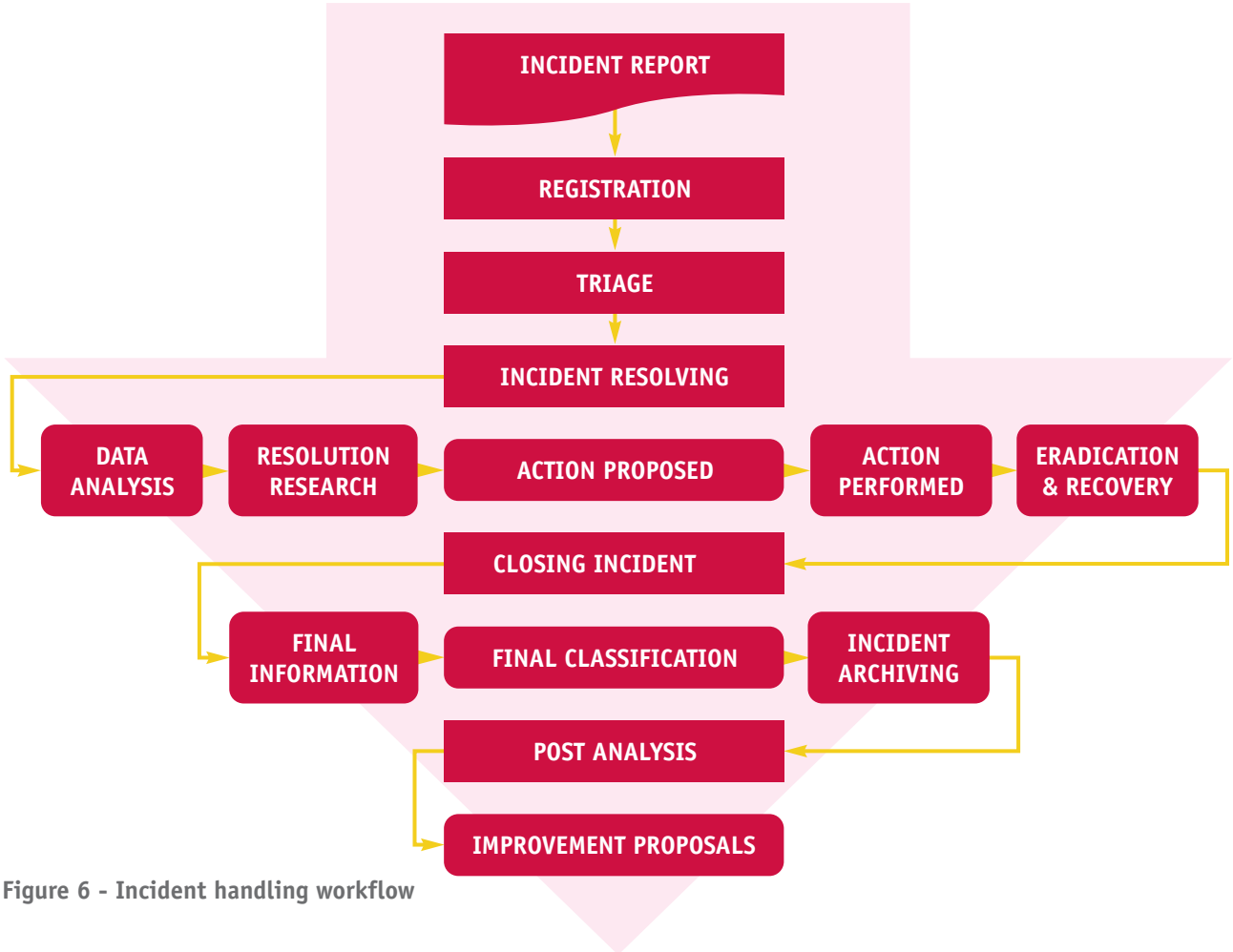


Figure 6 - Incident handling workflow

27 ENISA's exercise material home page: http://www.enisa.europa.eu/act/cert/support/exercise

Then, according to your preferences, you can develop either a list of guidance and advice notes for an incident handler (fixed to the particular phases) or a more advanced workflow with graphical representation of decision trees. See the diagrams below for some examples.

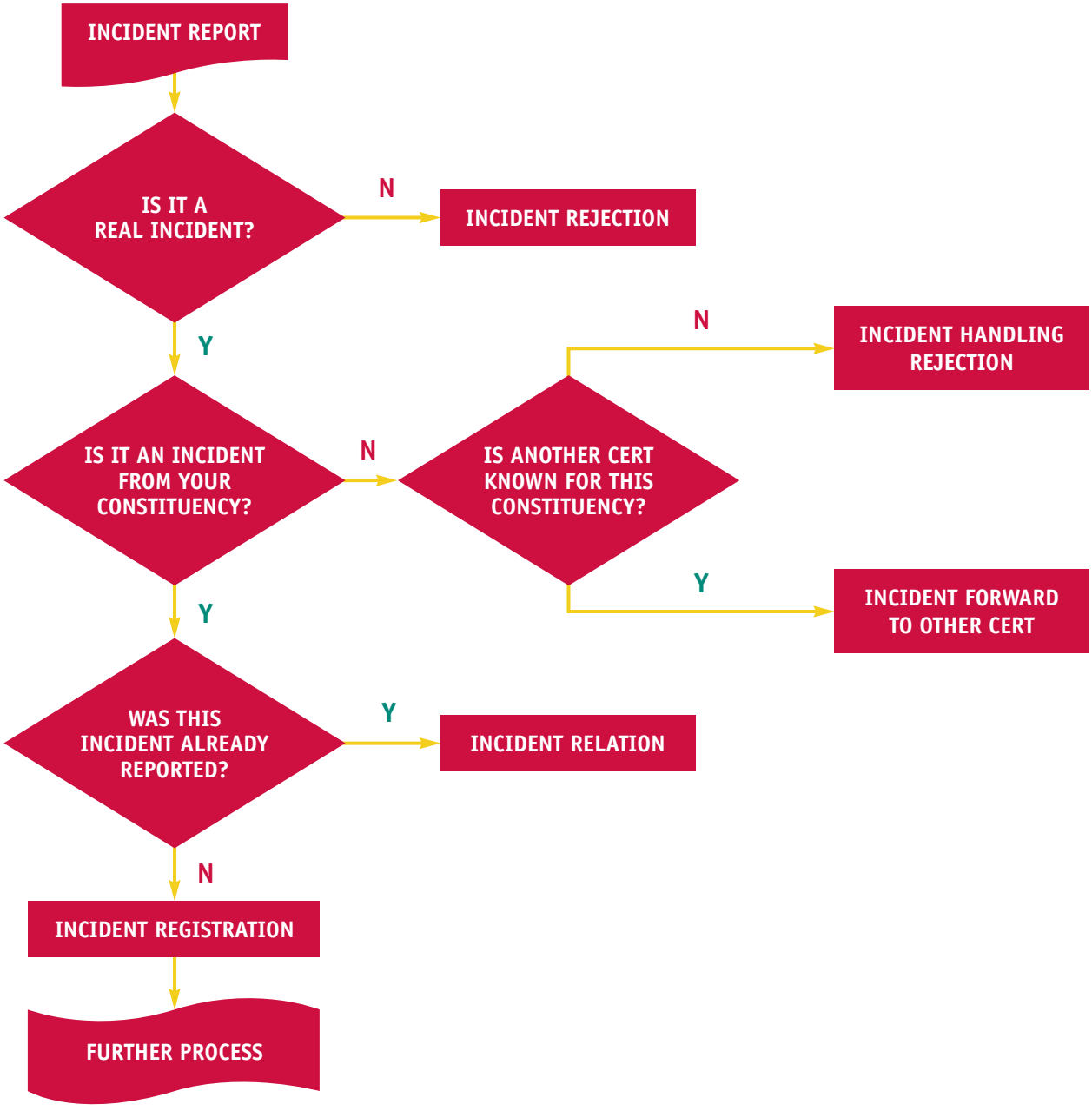
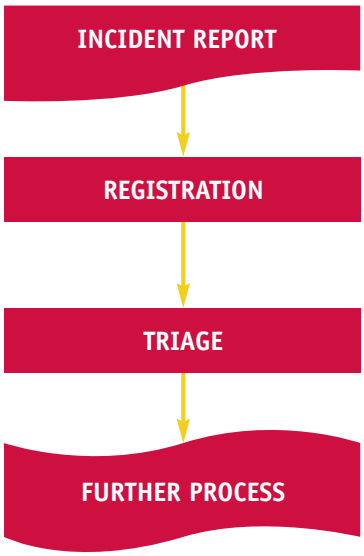


Figure 7 - Part of a detailed incident handling workflow – graphical approach



1. CHECK WHETHER IT IS A REAL INCIDENT?
   - **IF NOT – REJECT IT**

2. CHECK WHETHER IT IS AN INCIDENT FROM YOUR CONSTITUENCY?
   - **IF NOT – CHECK IF YOU KNOW ANOTHER CERT TEAM WHICH COULD HANDLE THIS INCIDENT AND FORWARD IT TO THEM**
   - **IF YOU DO NOT PASS IT ON – REFUSE TO HANDLE IT AND EXPLAIN THIS TO THE REPORTER**

3. CHECK IF THE REPORTED INCIDENT WAS ALREADY REPORTED TO YOUR TEAM?
   - **IF IT WAS – LINK THEM**
   - REGISTER INCIDENT
   - [FURTHER PROCESSING]

Figure 8 - Part of detailed Incident handling workflow – descriptive approach

From time to time you will have waves of particular types of incidents (eg, popular e-mail viruses, Internet worms or hacking techniques). Dealing with them usually allows you to develop a specific workflow in a very short timeframe, which can be most effective. In such cases, it is worth documenting this process in order to have it used by all team members. You can capture it as a short description of steps that must be undertaken or as a graphical workflow. In general these descriptions or checklists are called *cheat sheets*[28].

7.2 Method of presentation

You need to decide how you are going to present a workflow to your team members. You can do it in many ways, for example:

- Hang it on a wall, in the most visible place in the office.
- Print it and hand it out to each team member.
- Create advice or guidance notes (or even introduce a rule) and keep them in a place that is easily visible to every incident handler.
- Embed it in your incident handling system
  - simply – displaying a workflow as a picture
  - intelligently – fixing it to the real workflow.

If it is produced in high quality using good graphic design, hanging the workflow on a wall in the office will help your team members to identify with the process and this is a good way to show other colleagues what your team does.

Whatever method you choose, your ultimate success and that of the team depends on how good and practical is the incident handling procedure you have developed.

28 Some cheat sheets can be found at: http://zeltser.com/cheat-sheets/

7.3 How to use the workflows in daily work

In the last section you considered how to present your workflow. Now you need to consider how to use it as part of the daily work routine. Generally speaking, incident handlers, at least some of them, have nothing against the introduction of rules that structure part of their thinking about a problem. However the workflow you have defined does not have to be set in stone for all time. Over time it will deviate from the rules as new situations arise. The main reason for this is that the workflow is no longer up to date and it does not correspond to the actual needs. So remember to keep it updated. To achieve this periodically you can repeat the process of workflow development described in section 7.1 Proposed workflows. Advise your team members every time you change something in the workflow and there is a new specific procedure to deal with specific reports or incidents.

The best way to ensure that your incident handlers follow the agreed workflow is to implement the workflow in the incident handling system. Unfortunately there is no known off-the-shelf pre-configured system you can deploy. However, if you have the capabilities, as many large organisations do, the workflow could be implemented in the trouble ticketing and management system used by the organisation.

In order to convince your team to have a positive approach to using the workflow, you can explain that:

- Following the workflow makes your procedure and activity clear to you and to every party with whom you are cooperating.
- Following the workflow helps you resolve an incident faster and more effectively. The workflow is a result of the work of all team members and, as a group, you know the best way to do it.
- Following the workflow makes your team work easier. Every incident handler can easily determine in which stage an incident is and what to do next.

Keep the incident handling workflow alive and up to date. It may not be obvious but it does underpin your service and can improve it.

7.4 Incident lifecycle

During the incident handling process, it is beneficial to know in which phase of the incident lifecycle you are. To be able to know this, you need to define all the phases. There may be many different proposals for doing so. Please consider the ITIL (IT Infrastructure Library)[29] incident lifecycle for your internal use. It is presented below.

29 What is ITIL?: http://www.itil-officialsite.com/AboutITIL

The ITIL incident lifecycle consists of the following phases[30]:

- occurrence – an unplanned disruption to an agreed service;
- detection – a process which occurs sometime after the occurrence of an event;
- diagnostics – identification of the characteristics of the incident;
- repair – a process of reconfiguring attacked items;
- recovery – a process of restoring the failed items to their last recoverable state;
- restoration – a process of providing an expected service back to a user;
- closure – the final step in the incident lifecycle, during which a user and an incident handler check that a service is fully available.

Are there any practical benefits related to the fact that you know these phases? The answer is 'yes' but only if you monitor them. The primary benefit is that, following these phases, you can be sure that you do not omit an important part of what you have to do.

Another purpose of observing the incident lifecycle is to improve the effectiveness of your service. To do this, first you should measure the duration of the particular phases and then:

- find the longest phases and try to shorten them if you find them unjustifiably long;
- look for changes in duration, and identify and stop any unjustifiable increase in their duration[31].

If you identify the need for improvement and decide to undertake steps to improve your incident handling process then monitor the implementation of the improvements and check whether they bring the desired results. Decreasing the time of particular phases should not be an aim in itself.

How to measure incident lifecycle phases?

There is no easy way to do so. One method would be to observe the time-stamps of your e-mail correspondence for particular incident handling phases, eg, incident report mail, your notification e-mail, incident closing e-mail, etc. A helpful tool for doing this can be your ticketing system for incident handling. It can automatically change and record status.

As a result of your analysis you can, for example, easily observe that there are relatively big time gaps between your e-mails during an exchange of correspondence – and you may want to address this.

30 Expanding the Expanded Incident Lifecycle: http://www.itsmsolutions.com/newsletters/DITYvol5iss7.htm
31 eg, by using the 'Automation in Incident Handling' exercise from the ENISA *CERT Exercises Handbook* http://www.enisa.europa.eu/act/cert/support/exercise/

INCIDENT HANDLING PROCESS

8 – Incident Handling Process

The incident handling process has many phases. It describes the sequence of steps that begin when an incident reaches your team. It could follow a very simple or very sophisticated model. Start planning your incident handling process with a simple set of tasks and subsequently expand it to new ones according to your real work and needs[32].

You can use the set of tasks discussed below as a framework for your incident handling procedure. This is the same set of tasks that form the workflow shown previously in Figure 6. Practically every incident handling procedure should consist of these tasks. It is up to you how much you will develop them and how much more detail you will go into.

Good practice is to start with the simple model and then, as you and the team become more experienced, develop the procedure further.

8.1 Incident report

The CERT receives a report about an incident, which can reach the incident handling system via many means of communication: e-mail, fax, phone call, snail mail, walk-in report, and website form. Usually, most teams want to consolidate the reporting channels. The most common way to do so is by e-mail. You may prefer to get incident reports via your website incident reporting form; however experience shows that this can not be relied upon as people do not like to use that channel. They prefer to simply send an e-mail. If you have automated incident reporting or you are planning to introduce this in the near future – e-mail is probably one of the easiest means of communication to link to your incident handling system.

The methods presented above are reactive ones, relying on a third-party to raise the alarm. This is good way to start. But if you have sufficient resources, you can also approach this more pro-actively. With appropriate systems you may be able to detect incidents in your network and move them to the incident handling lifecycle. Here are a few methods for doing so:

- Subscribe to services which provide information about compromised machines from your constituency[33].
- Use your network monitoring systems (eg, intrusion detection systems or any other threat monitoring systems) to actively look for incidents in your network.
- Monitor blacklists for records from your constituency.
- Cooperate with others who actively monitor their networks and ask them for data related to your constituency (the best option is to exchange data as the win-win approach is potentially the most effective). Using monitoring systems to actively search for the signs of incidents will help your team to follow up with all newly discovered breaches. It is good practice not to work only with reports sent to you by others.
- Monitor forums and news websites for possible incident reports or threats. A constituent is not always aware that he is experiencing a security incident, but they might suffer downtime or slow service, which is then noticed by the press or results in questions or discussions in forums.

32 To learn more about how to do this - see chapter 7 Workflows.
33 eg, http://www.zone-h.org/

8.2 Registration

A report is formally registered in your incident handling system. This should be linked to some alphanumeric reference so it can be easily managed in the future. For example, the naming scheme can be [*CERT-NAME# report_number*]. Most incident handling systems can do this automatically. It makes subsequent and further incident processing easier.
If you find that an incident report is related to an already-registered incident you can decide to link or combine them together.

You should consider that your incident handling system is very similar to any other e-mail account. It should be protected again spam. Otherwise you can expect a significant additional workload in managing it. This stage is also the best one in which to implement any pre-filtering mechanisms (eg, for moving special kinds of incidents to a particular place or folder in the incident handling system).

Use of an incident report registration form could facilitate the registration process. There is no standardised form used by CERTs. Most of them have their own forms adjusted to their own individual needs (eg, their taxonomy)[34]. A form can be placed on your website as an HTML or plain text form.

Before you decide what the incident form should look like, it is a good idea to study at least a few existing ones[35].

When using a web-based form on your website, please take the appropriate measures to protect yourself and the incident reporter from any leakage of the incident report or the receipt of many inappropriate reports.

8.3 Triage

The name triage comes from a French medical term, which describes a situation in which you have limited resources and have to decide on the priorities of your actions based on the severity of particular cases. In the incident handling process, the triage phase consists of three sub-phases: verification, initial classification and assignment.

To implement triage in your incident handling process, you can consider your incidents in the same way a doctor thinks about patients. You will need to complete the triage process to prioritise the incident and progress it to diagnosis and resolution. The triage should determine the:

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

34 Study IODEF (Incident Object Description and Exchange Format) to finally decide the set of information you want to collect via your incident reporting form: http://xml.coverpages.org/iodef.html
35 The proposed examples are: the US-CERT form: https://forms.us-cert.gov/report/, the BELNET CERT form: https://cert.belnet.be/content/report-incident, the CERT.at form: http://www.cert.at/static/form.txt, and the FORTH CERT form: http://www.forth.gr/forthcert/report-online.php

The basic questions that should be answered in this phase are:

- Is it really an IT security incident?[36]
- Is it related to one of your constituents?
- Does it fit within the mandate the CERT has?
- What is the impact?
- Is there collateral damage?
- How fast could it spread to other constituents?
- How many people do you need to handle this incident?
- Which incident handler should be appointed to the incident?

This information allows you to decide what to do. Should you reject the incident, should you undertake immediate action or can you perhaps handle the incident later? You can also decide that just advice is enough at this moment because the incident was reported by an experienced user (you know him). Eventually you may skip handling completely if your triage process tells you the issue is not important at all.

8.3.1 Incident verification

At the verification step, a report is examined as to whether or not it concerns a real incident. Sometimes inexperienced incident reporters can send, for example, a system notification (eg, mail server report that your e-mail was not delivered). If it is a single isolated case, you can respond kindly to such mis-reports but if there are a lot of them it consumes your resources. So the best way to save time is to reject the handling of such a report. You do not have to put extra energy into answering these reports – the solution could be an appropriate text in your automatic reply, which you send to incident reporters. Also, considering that your incident handling inbox can contain a lot of information and queries about scanning activities or network probes, it is almost impossible to handle all of such reports fully.

Good practice is to answer with some explanation of what scanning or probing is, why you do not handle it, and what to do to avoid successful attacks on the network of the incident reporter. This can also be a good method for building awareness within your constituency. Do not miss any opportunity to create more awareness. It is, however, wise to archive all of the reports you reject, as one of them could lead to an incident or be useful information for other incidents.

Also check if it is 'your incident' (within your mandate or constituency). If it is, it can be further analysed and handled; if not, it can be rejected or forwarded to another CERT with responsibility for the constituency from which an incident comes.

As a general rule you should react at least once to an incident report. This can be done by developing an auto-response mechanism. Every mail reaching your incident handling inbox will be answered in automatic way. In the response you can include information such as:

- acknowledgment that notification of an incident was received;
- minimum information about what will happen to the report;
- what the incident reporter can expect as the next steps.

36 If it is not an IT security incident, you could still need to handle the incident report, as in the case of a potential vulnerability, but this is outside the scope of this document.

The textbox on the side shows the example of an auto-response.

If you plan to not answer the reporter of a rejected incident, consider including information about the types of incidents being rejected in your auto-response message and clearly state that a reporter of such incidents should not expect any further correspondence.

Reject an incident report when:

- it has nothing to do with your constituency;
- an incident reporter expects services from you that you do not deliver;
- it is not an incident, or not one by your definition at least.

Ignore an incident report when:

- it has been reported anonymously or by an untrusted or unreliable party, eg, you had reports from them before that proved to be false.

CERT POLSKA AUTORESPONSE

Hello,

Your report has been received and an incident investigation has begun according to our procedure. In some cases it may be necessary that we contact your system administrators, other incident response teams or law enforcement about this issue. Note that we never share information about the reporter, or the constituent involved, unless specifically authorized.

We will contact you only if necessary. Should you decide to contact us again about this issue, please include the following ticket id: [{$rtname} #{$Ticket->id}] in the message subject or quote the number during a phone call.

Best regards,
CERT Polska

8.3.2 Incident initial classification

After verification, you can initially classify an incident. It is classified according to your classification schema. To decide how the incident is to be classified, you try to determine as much information as possible from the report (and possibly other known reports). This is not an easy task as, at this stage, you usually do not have enough data to do it properly. Nevertheless it is important to classify your incidents at this stage[37].

8.3.3 How to prioritise actions within your constituency

Sooner or later you probably will not be able to manage every incident at the highest level of your effectiveness. You will be forced to differentiate your level of service. So you will have to divide your constituency into different categories according to your prioritisation. While doing so you have to keep your 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.

37 For more information on how to do so, you can read section 8.7 Incident taxonomy.

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

Let's look at the following example. Assume that you are a CERT that, according to its mission, should protect a public administration (generally under a .gov.<country> domain). Additionally, you have some commercial contracts with financial institutions to provide them with an incident handling service (service level agreement contracts). Finally, you have divided potential incidents into three groups, according to their severity:

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

Table 9 - Basic prioritisation of incidents by severity of attacks

Your potential solution to prioritise incident handling could be a matrix showing a combination of the importance of your customer and the severity of the attack.

PRIORITY	.GOV ORGANISATION	SLA CUSTOMER	OTHERS
RED	1	1	2
YELLOW	2	1	3
ORANGE	3	2	3

Table 10 - Basic prioritisation of incidents by type of constituency member

For practically all your SLA customers you deliver a priority 1 service – that is the highest priority. As you did not contract for such a service for your .gov constituency, you do not have to deliver such a service to them. You only react with the highest priority to the most severe incidents. For the rest of your constituency you deliver a 'good effort' service with special care for incidents of severity RED.

8.3.4 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 specialised handlers for particular types of incidents (eg, spam or malware), or finally you can have an incident handled by more than one handler according to their availability, specialisation or other factors.

8.4 Incident resolution

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.

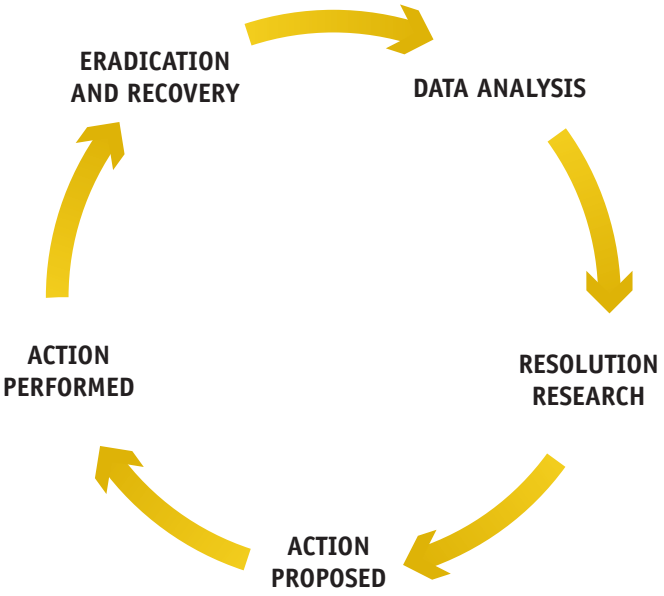
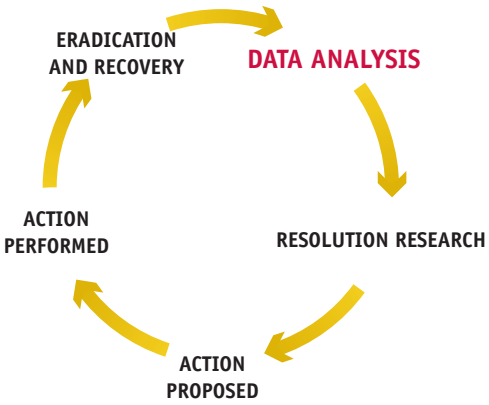


Figure 9 - Incident resolution cycle

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.

8.4.1 Data analysis



To start data analysis, first you have to notify the parties involved and collect data from them. 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. There are several main sources of such data:

- Incident reporter – depending on how much information was given in the initial report you should ask for additional data you need, such as:
  - detailed contact information
  - detailed description of the incident
  - incident classification suggested by the incident reporter
  - logs
  - the exact time of the incident
  - operating systems and network setup
  - security systems setup (eg, antivirus software or firewall)
  - incident severity (in the incident reporter's opinion).
- Monitoring systems – try to search for information related to the IP addresses involved in your network monitoring systems (eg, netflow database).
- Referring database – check if this kind of incident or this incident reporter are already in your incident database. By doing this you can learn a lot and speed up the resolution of the incident.
- Other sources – relevant log-files (routers, firewalls, proxy servers, switches, web application, mail servers, DHCP servers, authentication servers, etc).

The target of attack and the incident reporter do not have to be the same party. Sometimes a target does not know that he is being attacked. In such cases your information is very important as it allows an attack target to learn about his situation and to mitigate the threat. Of course you also try to determine the source of the incident. To be successful at the latter task, you should contact as many relevant parties as possible.

These parties – the attack target, ISPs involved, including on both attacking and attack target sides, or internet content provider (ICP), law enforcement agencies (LEA) – can help you to collect the necessary information related to your incident. In practice, solving the incident is practically impossible without involving many or all of these parties. Contacting them and working with them may require many repeated activities. Sometimes contact is easy and a party is very responsive and helpful, while at other times you have to be really persistent in order to obtain a single piece of information that is vital to you or convince them to take some action. To get the support you need, use the following arguments:

- Giving information provides an opportunity to improve the security level of many organisations and individuals.
- An incident can result in a real legal case – it is worth taking effective steps towards its mitigation and the proper collection of evidence about the incident.

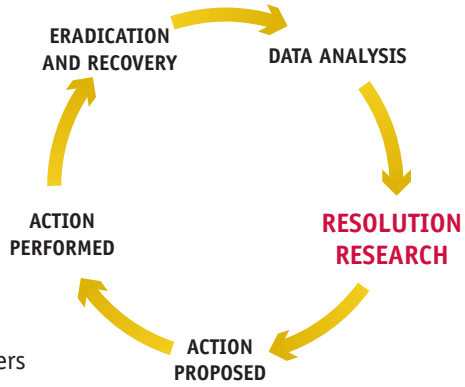
Usually, using negatively-oriented arguments such as 'you must do it because it is your computer that does bad things' does not work. Sometimes it is your last resort. An argument that you will be forced to contact the management of an uncooperative party can work; by the way, this may be part of your defined incident handling procedure.

Having completed the notification and data collection tasks, you can now start data analysis. Your success very much depends on this part. You have collected data and now you have to decide which data to analyse 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?

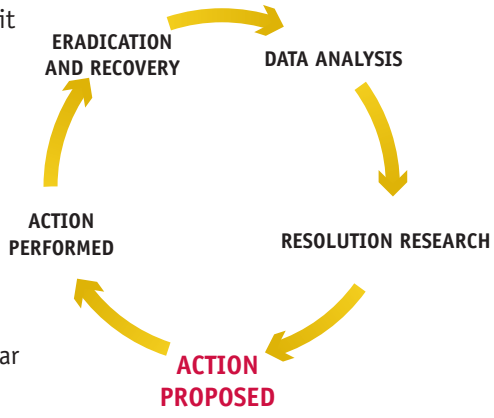
Then you can start the work of data analysis. It is important to distribute this work properly within the team. In general, consider two factors: a team member's expertise and a team member's current workload. Adjust your action plan to take these factors into account.

8.4.2 Resolution research



Very often during the data analysis phase people exchange their ideas, observations and draw conclusions. This means that your team has practically entered the resolution research phase. The ideas people propose during these 'sessions' are usually very valuable but the problem is that hardly anyone makes proper use of them. The ideas are broadcasted in an office and only a few of them, if any, are implemented in practice. This is a kind of specific brainstorming session, so you need a way to avoid wasting and losing this valuable information. The solution is simpler than you may expect – just advise, convince or order team members to collect any observations they make by writing them down on a sheet of paper. Then you can hold periodic review sessions (eg, every day or every two hours for very urgent incidents) and exchange, discuss and decide which ideas you will use for the resolution of the incident. Also try to avoid the pitfall of perfectionism. Sometimes you feel that you have to collect and analyse much more data to be sure that you have done everything to be successful. 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 your reaction. Sometimes a quick response has the same or a higher value than a comprehensive and complete set of information.

8.4.3 Actions 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 (eg, 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. Below are some examples of actions you can propose to particular parties:

- Attack target
  - How to stop and mitigate an ongoing attack:
    - turn off a service
    - check the system for malware
    - patch a system or an application
    - perform or order an audit if you are not able to improve your system security yourself.
    - How to deliver more data:
    - concrete practical instructions (eg, how to obtain a full e-mail header); having some of your most often used instructions ready and available on your website is good as then it is enough just to point links to them.

- ISP/ICP
  - To collect, save and archive data. Some of this data can be available without any special restrictions; other data requires special protection (eg, personal data) – in this case all you can ask for is for the data to be saved so that it is available if the target of the attack reports a case to the police.
  - To monitor network traffic related to the case and inform you if something important happens.
  - To filter network traffic in the case of an ongoing attack if such filtering can help to stop or mitigate it.

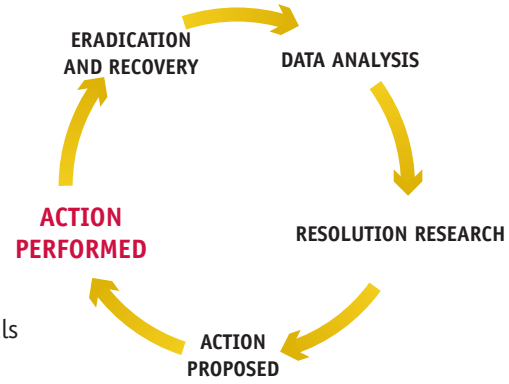
- CERTs
  - To contact the local ISP/ICP within its constituency. Usually contacting an ISP/ICP which is outside your constituency, especially in other countries, through the relevant CERT will work much better than your direct probes.
  - To ask for advice on how to deal with an incident where a similar incident happened to this CERT. It is good practice to use trusted information distribution channels such as the TERENA TI mailing list or FIRST mailing list[38].

- Law enforcement agency (usually the police):
  - To follow a case if it is significant (eg, you suspect organised crime activity)
  - To assist the reporter of a crime if an incident is to be reported to the police[39].

- Source of an incident (the attacker)[40]
  - To advise and propose similar actions to those given to the attack target (see above).
  - DO NOT contact the source of the incident if you seriously suspect that you may be contacting a real criminal. Giving information that somebody is aware of a crime could decrease the effectiveness of the investigation. In such a case it is highly recommended that the incident handling is coordinated with an LEA.

38 You can become a subscriber to these lists by becoming a member of these organisations. Learn how to become a FIRST member at: http://first.org/members/; learn how to become a Trusted Introducer team at: http://www.trusted-introducer.nl/ti_process/.
39 In most legal systems, a crime should be or even has to be reported to the police by the victim, so your role is to convince victims to report a crime. It is part of your ongoing effort. Most victims are not interested in reporting a crime for many reasons (eg, they do not believe that the police will be able to find the criminal). Do not give up – statistically your effort will improve the situation (eg, more reports to the police are a signal that an LEA should significantly improve their investigative capabilities).
40 ie, a party which turned out to be the attacking side, but usually did not know this, as his or her computer had become a tool in the offender's hands.

8.4.4 Action performed



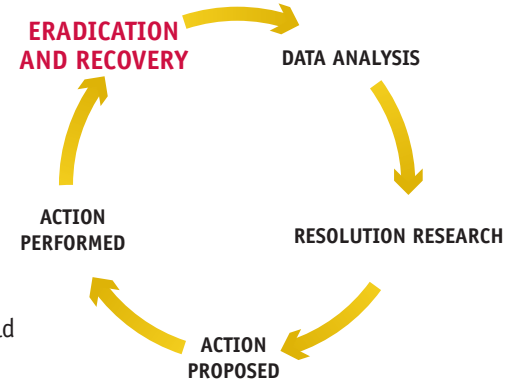
Whatever in your plan is identified as your action – it is your decision as to whether it will be carried out or not. You have limited power to decide what others will do. It is a rather optimistic assumption that all, or even most, of your proposed actions will be executed by other parties. In practice this will not happen. Parties to whom you propose or ask to do something are out of your direct control. The only exception is where you are an internet service provider's CERT and in the user-rules for your customers it states that if they do not act appropriately on your proposals then you are allowed to limit their internet access.

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.

8.4.5 Eradication and recovery



All your actions have one main goal – the eradication of the incident.

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.

If you have doubts that you eradicated a problem and recovered a service, it is good practice to check yourself as much as possible and/or get a positive confirmation from each party that in their opinion everything is operating normally again.

8.5 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.

8.5.1 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:

- an attack target (very often a reporter of the incident);
- the most important parties involved in resolving the incident, who are usually ISPs/ICPs, other CERTs, and LEAs;
- a source of the incident (an 'attacker'[41]).

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.

The last point should be tailored to the party to whom you are sending your information. Do not send the same information to a typical internet user who reported a problem and the advanced technical staff of a CERT. Remember that handling an incident, whether it was successfully resolved or not, provides a valuable lesson for you and your contributors. So you can:

- teach the attack target what has happened and how to avoid such a problem in the future;
- explain the mechanism of the incident to the ISP/ICP to help them improve the security of their infrastructure;
- share the root cause of the incident with other CERTs;
- develop effective cooperation and procedures with the LEA involved;
- teach the party that was a source of the incident how to avoid being an 'attacker' in the future.

8.5.2 Final classification

If you pay attention to the classification of your incidents, you should analyse carefully when to finalise 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.

41 ie, a party which turned out to be the attacking side, but usually it did not know this, as his or her computer had become a tool in the offender's hands.

That is the theory. In practice, classification is very often treated by incident handlers as an unnecessary task that has no special meaning or value. They understand the complexity of a case and the difficulty of providing unambiguous results for the classification.

GOOD PRACTICE

So good practice is to minimise the work related to this task and apply a simple rule on how to do it. It is of greater value to have a simple and repeatable procedure, which ensures that all incidents of the same type will be classified in the same way, rather than a sophisticated procedure that delivers different outputs in the end.

So the possible options for you are to:

- classify incidents according to what is reported by incident reporters;
- classify incidents according to what is recognised by incident handlers at the very beginning of the incident handling process.

SUGGESTION

Classifying incidents at the end of the process seems to be tempting but is not recommended. Many incidents are handled by more than one incident handler, so no one may have the final overall information about the incident. Additionally, the complexity of the process tells you that this is not a simple solution for classification. It could become paralysing.

8.5.3 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.

In relation to the protection of archived data, you should especially consider their encryption and backup.

GOOD PRACTICE

Additionally, if your data relates to internet traffic data, 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[42]. You have to follow the law related to this problem.

After a period of legal data archiving, you must destroy that data. Remember to do so using effective data erasing algorithms.

42 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT

8.6 Post-analysis

The process of post-analysis starts after incident resolution or closure. Carrying out this process is difficult because there is natural resistance to it from incident handlers. They feel they have done everything they could and nothing new can now be learned. So good practice is to wait until some time after an incident is closed before you start post-analysis. During this time you can forget about the incident and then look at it with a fresh mind, and/or you can learn from other sources about this kind of incident (eg, somebody will issue his or her report on an attack mechanism).

Not every incident is worth analysing. Choose the most characteristic ones, the most complex, and those that include new attack vectors.

AN EXAMPLE OF AN AGENDA FOR AN INCIDENT HANDLING TEAM'S PERIODIC POST INCIDENT MEETING (eg, bi-weekly)

a. Information on incident data statistics for the last two weeks
b. Short (5 minutes) presentation about the 3 most interesting incidents (presented by various team members)
c. A detailed analysis of one chosen incident (previously chosen by team members).
d. Discussion:
- **lesson learnt session,**
- **brainstorming session for further proposals for improvement.**

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 organised periodically and systematically, they can be an important and valuable part of your team's professional life.

8.6.1 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.

Who can benefit from this? Use the same set of parties with whom you collaborated or contacted during the resolution of an incident (see section 8.4 Incident resolution). Try to take advantage of what you have learnt from incidents that came to your team for resolution. This is usually very valuable material that can be used effectively in your awareness-building activities. So, you can:

- teach an attack target how to:
  - collect all available logs
  - describe an incident
  - avoid similar incidents in the future;
- advise and teach internet service providers and internet content providers how to:
  - retain logs for further investigation
  - assist your team or other CERT teams in an operational action;
- explain the ISP/ICP mechanisms of the most important incidents and how to systematically handle them;
- support other CERTs with ideas on how to:
  - mediate between CERTs and local ISPs/ICPs
  - share advice and experience in resolving particular kinds of incidents;
- support law enforcement agencies with:
  - your opinion about the effectiveness of legal aspects (you can even provide your ideas for further legal actions or/and amendments to the existing law)

- advise a party which is a source of incident (an 'attacker'[43]) how they can in future:
  - monitor the security of his/her information resources
  - search for suspicious users of his/her information resources
  - avoid being a source of an incident.

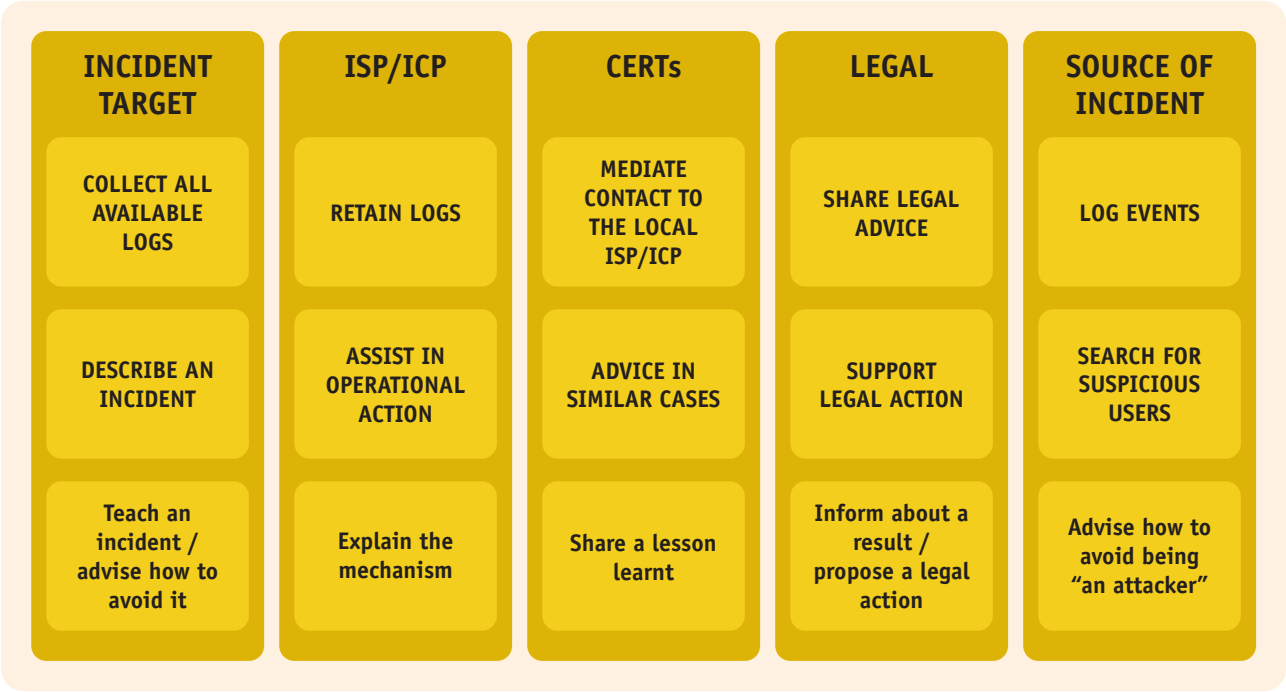


Figure 10 - Examples of improvement proposals for involved parties

8.7 Incident taxonomy

Incident taxonomy is a controversial topic. The simple question is – is it worth having an incident taxonomy and classifying incidents according to the taxonomy or not? As you can expect – there is no simple answer to this question. There are many pros and cons. Let's look at them before you make a decision on what to do.

43 ie, a party which turned out to be the attacking side, but usually did not know this, as his or her computer had become a tool in the offender's hands.

PROS	CONS

● systemisation and regularisation of work
● an opportunity to produce statistics
● an opportunity to observe trends
● a means of communication with:
  ○ management
  ○ the media
● a common language for naming threats
	● an increase in the complexity of incident work
	● an increase in the duration of incident handling
	● not a real picture of internet threats
	● the difficullty of ambiguous classification

Table 11 - Pros and cons for incident taxonomies

Ultimately it is your decision but having a taxonomy and classifying incidents in accordance with it is recommended. This recommendation is not made because there are more pros listed than cons. These lists represent just a fraction of the pros and cons under discussion. The real value of having a taxonomy is that you have at your disposal a quite effective method for developing your awareness services. All statistics, observations of trends, etc, which have their origin in a CERT taxonomy give you the capability to provide information about the most important topics in your constituency. Also, in this way, you can interest the media, who are your best information brokers. Last but not least – an information taxonomy and a classification based on it are very good tools for keeping management informed.

It is true that some team members do not understand this, especially technical staff, but there is no question that the values mentioned above does exist.

8.7.1 Existing taxonomies

Generally speaking, existing incident taxonomies belong to either of the following groups:
- specific taxonomies developed by individual CERTs
- universal, internationally recognised taxonomies.

As examples of the first group, consider the taxonomies used by two European CERTs.

The first is the taxonomy developed by the Latvian CERT NIC.LV[44] team. It consists of eleven types of internet security attacks:
- attacks on the critical infrastructure
- attacks on the internet infrastructure, eg, root or system-level attacks on any server system, or any part of the backbone network infrastructure, denial of service attacks
- deliberate persistent attacks on specific resources, ie, any compromise which leads or may lead to unauthorised access to systems

44 CERT NIC.LV team website: http://cert.nic.lv/

- widespread automated attacks against internet sites, eg, sniffing attacks, IRC 'social engineering' attacks, password cracking attacks
- threats, harassment, and other criminal offences involving individual user accounts
- new types of attacks or new vulnerabilities
- botnets, ie, activities related to the network of compromised systems controlled by a party which is the source of an incident
- denial of service on individual user accounts, eg, mail bombing
- forgery and misrepresentation, and other security-related violations of local rules and regulations, eg, e-mail forgery, SPAM, etc
- compromise of single desktop systems
- copyright violations.

This kind of taxonomy was probably established according to the team's experiences. In general, it corresponds to what a team receives as incident reports.

The next taxonomy is different. It is short and is based on completely different factors. This time you see a taxonomy which corresponds to who reported an incident. It is used by CERT-Hungary team and it consists of only four categories:

- national CIIP
- CIIP of partners with SLA
- incidents reported by international partners
- threats and incidents reported by cooperating organisations.

If you look further into proprietary taxonomies, you will find more variations. Their value is that they maximise the correlation with a team's needs and expectations, but they are not universal or directly comparable with other taxonomies. This means they can be used for your own internal requirements but comparison with other similar teams will be almost impossible.

To be able to compare, you should at least try to use one of the open models used by more than one team. One in particular is worth considering. Before that is presented, first a glance at one of the oldest schemas, which was developed at the Sandia National Laboratories and is called 'the Common Language'[45].
In this taxonomy, there are three main terms:

- event
- attack
- incident.

45 *A common language for computer security incidents* – John D Howard, Thomas A Longstaff http://www.cert.org/research/taxonomy_988667.pdf. In this report you can also find information about more examples of the taxonomies of computer security incidents.

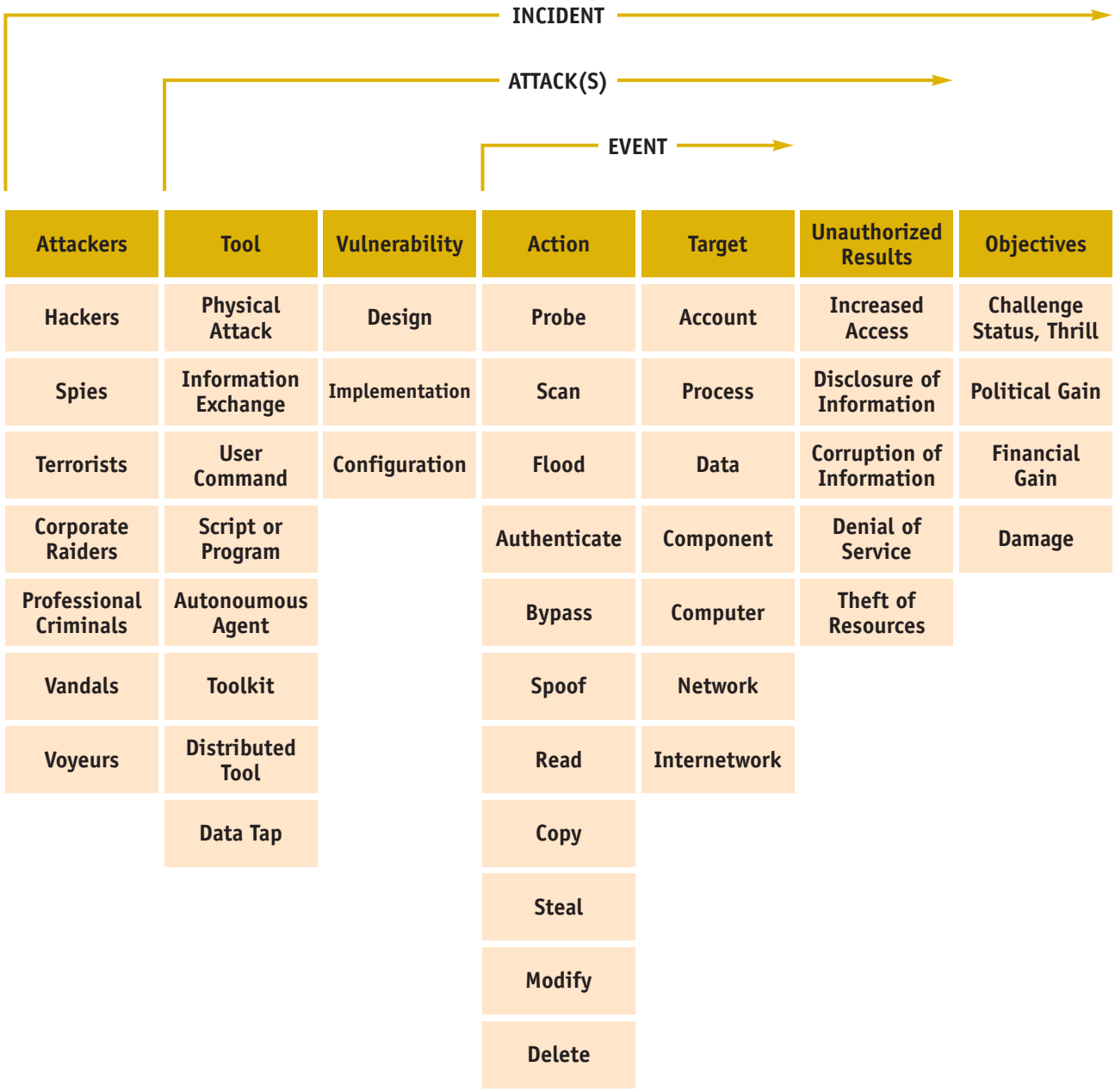


Figure 11 - Common Language security incident taxonomy

An event is when you have available information about a target of the attack and an action undertaken against it. When you have more information about it – a tool which was used in the attack, a vulnerability attacked and a result of the attack – then you can say that you have full information about the attack. According to this taxonomy you have an incident only if you collect all possible information so, besides the information about the attack, you should know who was the source of the incident and what was the objective of this attack.

SUGGESTION

As you can see this taxonomy is quite extensive. You have to makes decisions about seven different factors to be able to say that you have identified and classified your incident. It is complete. It gives you a chance to classify every incident in a very detailed way, but at the same time it is very time consuming and very often ambiguous. What is more – in most cases you do not have a chance to make use of this fully-detailed description, because you are not able to collect all the information needed. It is worth using, however, for research purposes, theoretical considerations and for creating your own taxonomy.

The second taxonomy that is worth knowing is the taxonomy popularised within the European CSIRT Network project – eCSIRT.net[46]. The taxonomy used in this project is essentially based on the taxonomy of a Swedish CERT team – TS-CERT[47]. The table below presents the full classification schema of this taxonomy. It has eight main categories and twenty-five sub-categories.

Incident Class *(mandatory input field)*	**Incident Type** *(optional but desired input field)*	**Description / Examples**
Abusive Content	Spam	Or 'unsolicited bulk e-mail', meaning that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having identical content
	Harassment	Discrediting or discriminating against somebody (ie, cyberstalking)
	Child/sexual/violence/...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This also includes some kinds of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...).
	Sniffing	Observing and recording network traffic (wiretapping)
	Social engineering	Gathering information from a human being in a non-technical way (eg, lies, tricks, bribes, or threats)
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (eg, buffer overflow, backdoors, cross side scripting, etc).
	Login attempts	Multiple login attempts (guessing / cracking of passwords, brute force)
	New attack signature	An attempt using an unknown exploit

46 The European CSIRT Network project website: http://www.ecsirt.net/
47 TS-CERT was known as Telia CERT/CC in the days when this taxonomy was developed by their team member Jimmy Arvidsson.

Incident Class *(mandatory input field)*	**Incident Type** *(optional but desired input field)*	**Description / Examples**
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by unauthorized local access.
	Unprivileged account compromise	
	Application compromise	
Availability	DoS	In this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYN- a. PING- flooding or e-mail bombing (DDoS: TFN, Trinity, etc.). However, availability can also be affected by local actions (destruction, disruption of power supply, etc).
	DDoS	
	Sabotage	
Information Security	Unauthorised access to information	Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information during transmission (wiretapping, spoofing or hijacking) are possible.
	Unauthorised modification of information	Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information during transmission (wiretapping, spoofing or hijacking) are possible.
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (eg, the use of e-mail to participate in illegal profit chain letters or pyramid schemes)
	Copyright	Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez)
	Masquerade	Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

Table 12 - eCSIRT.net security incidents taxonomy

This taxonomy is not ideal but it has many factors which make it very useful. In particular the main categories seem to be very practical and universal. Even though the taxonomy was developed many years ago, the main categories are still current and you can easily use them today. The subcategories are not so current and can lead to problems with how to classify an incident. It is not particularly useful any more to make a distinction between DoS attacks and DDoS attacks or to determine what is a 'privileged account compromise', 'unprivileged account compromise' or 'application compromise'. In practice, subcategories became a part of the description rather than a concrete schema for classification. Nowadays it is really difficult to determine if a particular malware is a virus, worm, Trojan, spyware or a dialler. The functionality of malware changes and the honest approach is to classify it all as 'malicious code'.

The eCSIRT.net classification is highly recommended. Despite some defects, it is still quite useful and good. Many European CERTs use it. If you decide to use it, it will give you the opportunity to team up with others later and be able to compare and merge statistics.

8.7.2 How to use a taxonomy

If you decide to use a taxonomy, you probably envision one you will be able to use forever and which will not cause any problems or additional work. Achieving this is not easy . If you use your own experimental taxonomy, based simply on report types which reach your incident inbox, sooner or later you will probably be dissatisfied with it. You will find new incidents which do not fit into the existing schema, some types of incidents will disappear forever, etc. The temptation to continuously change the taxonomy is quite strong. Think twice before you do so. Remember that one of the main reasons of having the taxonomy is to give yourself the opportunity of observing trends in incident security. To do so effectively, you should have a stable, long-term schema for classification. So if you really want to change it, consider a few things:

- Choose or build a new simpler taxonomy – fewer categories are better than more.
- Avoid categories which represent current phenomena – they can disappear within a year.
- Observe whoever systematically presents statistics – ask them for advice.
- Choose a taxonomy widely used by others – you will be able to more easily compare statistics with them.

THREE STEPS TO GET CONSISTENT STATISTICS

1. **Gather your team together. Hand out a set of 10 different incident reports. Ask everybody to classify them according to your taxonomy.**
2. **Discuss the results of step one. Point out incidents which made no problem for people. Point out those that were classified differently and discuss the reasons. Reach an agreement for the future.**
3. **Repeat steps one and two periodically (eg, quarterly) as well as every time new kinds of threats appear and you feel that they are not unambiguous in terms of their classification.**

If you changed your taxonomy and would like to have a continuous set of statistics, consider the possibilities of category mapping. For example, if you changed from the Common Language taxonomy to the eCSIRT.net taxonomy, you can map:

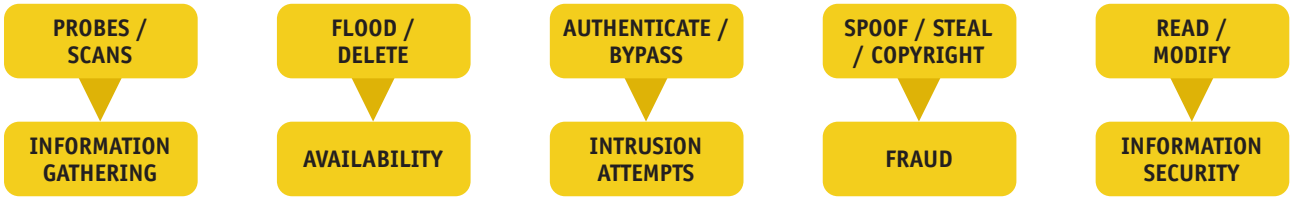


Figure 12 - Mapping incidents between different taxonomies

Another problem in the use of a taxonomy is having consistent statistics in terms of the same classification of the same kinds of incidents. If there is more than one person on your team who is responsible for incident classification, you can expect different results from this activity.

Use the proposed 'Three steps to get a consistent statistics' from the text box above to deal with this problem.

Additionally, it is very good practice to use the CERT exercise 1 – 'Triage and Basic Incident Handling' from the ENISA *CERT Exercises Handbook*[48].

Whatever you do, no matter how you train yourself and your co-workers in improving your classification skills, from time to time there will be an incident which you really do not know how to classify. It could happen, especially as internet threats become more and more complex and sophisticated. The only thing you can do in such a case is to decide how to classify the incident and consequently use this approach. It is possible that in the future you will learn more about this attack and you will be then able to decide clearly how you should classify it. The fact that you classified this incident in one way gives you a chance to automatically change all past incidents according to your new decision. Some additional information in the incident database (eg, the name of a virus or worm) will be very helpful in searching your database for incidents for which you want to change the classification.

8.7.3 Trend observations

As mentioned a few times before – one of the main reasons to have statistics is to have the ability to observe trends related to them. There is no special mechanism for doing this. Simply comparing a number of particular types of incidents year after year allows you to form your own opinion on internet security trends. For example – some years ago most of the reported incidents were probes and scanning; nowadays the situation has changed and there are not too many of these incidents. Instead, there are new dominant threats in incident security statistics, such as phishing attacks, illegal content, Trojan horses or DDoS attacks. These kinds of observations could be valuable not only for your communication purposes (with media and with a management), but could also be useful for appropriately balancing your resources in awareness activities or research projects.

Remember that in your security incident environment there may be some factors that will significantly affect your statistical data. Some of these are:

- People just stop reporting some kinds of incidents (eg, scanning or probes) because they start to treat them as a normal part of internet traffic.

CASE STUDY OF SERVICE IMPROVEMENT BASED ON TREND ANALYSIS

By observing statistics, the team noticed a significant increase in the number of phishing attacks in its constituency. They organised a team meeting and developed the following ideas for improving their services:

- **Two team members were to learn more about the current methods of phishing attacks and present the results to the other team members.**
- **They were also to develop simple scripts to handle phishing incidents, especially to automatically inform banks about incidents (24/7).**
- **They were to issue in the following month at least six news items about the threat and to develop a basic guide for bank customers – 'How to avoid a phishing attack', and a guide for web-server administrators – 'How to protect your site against phishing attacks'.**
- **They were also to contact friendly media and inform them of the increase in the threat and ask them to disseminate advice for bank customers.**

48 ENISA's exercise material home page: http://www.enisa.europa.eu/act/cert/support/exercise/

- Some automatic service for particular kinds of incidents ceases operation (eg, reporting scanning, spam or website infections).
- You start your own monitoring service which will feed your incident database with a large number of new cases.
- Your team is advertised in the media as a reporting point and people start to report more incidents (at least for a short period of time).

What can be done in such cases? There is nothing specific you can do about it. The most important thing is to be aware of it, to discover these circumstances and to explain them to everybody to whom you present your statistics (on your website, in your reports, etc).

8.8 Information disclosure

Trust in you as a keeper of sensitive information is crucial for your work. In your daily work you 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 organisation. 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.

CERT.at rules for information disclosure

CERT.at will cooperate with other Organisations in the Field of Computer Security. This Cooperation also includes and often requires the exchange of vital information regarding security incidents and vulnerabilities. Nevertheless CERT.at will protect the privacy of their customers, and therefore (under normal circumstances) pass on information in an anonymised way only unless other contractual agreements apply.

CERT.at operates under the restrictions imposed by Austrian law. This involves careful handling of personal data as required by Austrian Data Protection law, but it is also possible that - according to Austrian law - CERT.at may be forced to disclose information due to a Court's order.

You can help yourself when making the decision whether to disclose data or not, by asking yourself the following questions[49]:

- Is use or disclosure necessary?
- Does the action support legitimate interests?
- Are the data subject's interests protected?
- Is processing justified?

As additional good practice, consider publishing non-disclosure rules in your RFC 2350[50].

49 Questions come from the document by Andrew Cormac – *Incident Response and Data Protection* http://www.terena.org/activities/tf-csirt/publications/data-protection.pdf. In this document you will find much helpful information, including examples of justifications for data disclosure, which improve the activities of CERTs (malware analysis honeypot, forensics data from compromised machine, and flow data for detecting compromised systems).

50 RFC 2350 – *Expectations for Security Incident Response* http://www.ietf.org/rfc/rfc2350.txt is a fundamental document for describing your team, your rules and how you operate. Practically every CERT should have such a document prepared and available on its website.

Besides good practice on information disclosure – there are legal obligations stemming from national or international laws. Probably the most important of these are the laws relating to the protection of personal data. All your procedures must comply with these laws.

8.8.1 Traffic Light Protocol

In 2009 the international community of CERTs in Europe, as assembled in the Trusted Introducer[51], adopted an information sharing protocol that was, at that time, already in use between various governmental CERTs worldwide. It originally stems from the UK governmental organisation NISCC.

It is recommended that you adopt and use this protocol to make clear what others can do with specific information presented by e-mail, on the phone, in a meeting or by any other means of communication. The protocol is based on the 'traffic light' colours and is as follows:[52]

All CERTs can have their own system of information classification with associated rules, but they will at least recognise and support the following ISTLP (Information Sharing Traffic Light Protocol), following best practice in NISCC (UK) with widening acceptance in the CERT community.

NOTE that an 'Information Exchange' can be either in person, like a meeting of CERTs or of a CERT with their constituents, or a meeting of just a few security professionals together, but also an exchange in e-mail or over the phone or fax. The rules below apply to all of those. It is not an absolute recipe, but needs to be applied thoughtfully - the ISTLP serves the purpose of bringing more clarity in regards the rules of information sharing - it is not a purpose in itself.

RED	Non-disclosable information and restricted to representatives participating in the information exchange themselves only. Representatives must not disseminate the information outside the exchange. RED information may be discussed during an exchange, where all representatives participating have signed up to these rules. Guests and others such as visiting speakers who are not full members of the exchange will be required to leave before such information is discussed.
AMBER	Limited disclosure and restricted to members of the information exchange; those within their organisations and/or constituencies (whether direct employees, consultants, contractors or outsource-staff working in the organisation) who have a NEED TO KNOW in order to take action.
GREEN	Information can be shared with other organisations, information exchanges or individuals in the network security, information assurance or CNI community at large, but not published or posted on the web.
WHITE	Information that is for public, unrestricted dissemination, publication, web-posting or broadcasting. Any member of the information exchange may publish the information, subject to copyright.

Table 13 - Traffic Light Protocol categories

51 Trusted Introducer for CSIRTs in Europe: www.trusted-introducer.org

52 The version presented here is identical to the Trusted Introducer version of the v1.1 ISTLP - Information Sharing Traffic Light Protocol, adapted for the community of TI Accredited Teams by Don Stikvoort, Trusted Introducer director, on 11 November 2009, by courtesy of the ISTLP creator NISCC (UK) – only the direct reference to the Trusted Introducer has been generalised in the text.

8.9 Tools

8.9.1 Clearing House for Incident Handling Tools (CHIHT)

Within Task Force CSIRT organised by TERENA in 2000, the idea of collecting valuable CERT tools and guidelines was developed. Thanks to this initiative, a collection of tools used by various European CERTs now exists. The project is called 'Clearing House for Incident Handling Tools'. It has the unique value of providing information not only about the tools but also about those who are using them. So, if you want to choose tools to use in your team, you can ask for opinions from other CERTs. You can also ask these teams for support.

On the ENISA website[53] 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.

You can easily cross-reference these groups to your incident handling workflow, just by looking at their names. Some of these tools are internet services, eg, databases such as ARIN or RIPE where you can find the contact information of organisations and people responsible for managing networks and hosts that are related to your incidents. When looking for these contacts, look especially for an RIPE IRT object in the RIPE database. It shows information about the incident response team that takes care of the IP address for which you are looking.

Table 14 - Example of an *IRT object* for one of the IP addresses

```
irt:            IRT-CERT-POLSKA
address:        NASK
address:        CERT Polska
address:        ul.Wawozowa 18
address:        02-796 Warszawa
address:        Poland
phone:          +48 22 3808 274
fax-no:         +48 22 3808 399
e-mail:         cert@cert.pl
signature:      PGPKEY-553FEB09
encryption:     PGPKEY-553FEB09
admin-c:        TI123-RIPE
tech-c:         TI123-RIPE
auth:           PGPKEY-553FEB09
remarks:        emergency phone number +48 600 319 683
remarks:        timezone GMT+1 (GST+2 with GST)
remarks:        https://www.trusted-introducer.org/teams/cert-polska.html
remarks:        This is a TI accredited CSIRT/CERT
irt-nfy:        cert@cert.pl
mnt-by:         TRUSTED-INTRODUCER-MNT
source:         RIPE # Filtered
```

53 Clearinghouse for Incident Handling Tools: http://www.enisa.europa.eu/act/cert/support/chiht

A helpful tool for finding this kind of information was developed by the CERT Polska team. Its name is 'IP digger' and it is available on their main site[54]. Put the IP address in which you are interested into the search window and you will find the contact data of parties with whom you can get in touch to help resolve the problem.

Many tools listed in the CHIHT database are simply UNIX or Windows commands so, if you have a team member with experience in UNIX systems, you do not have to pay special attention to this part of the repository – just remember that system commands (including 'programs' such as *awk* or *grep*) can be very helpful tools in incident handling work.

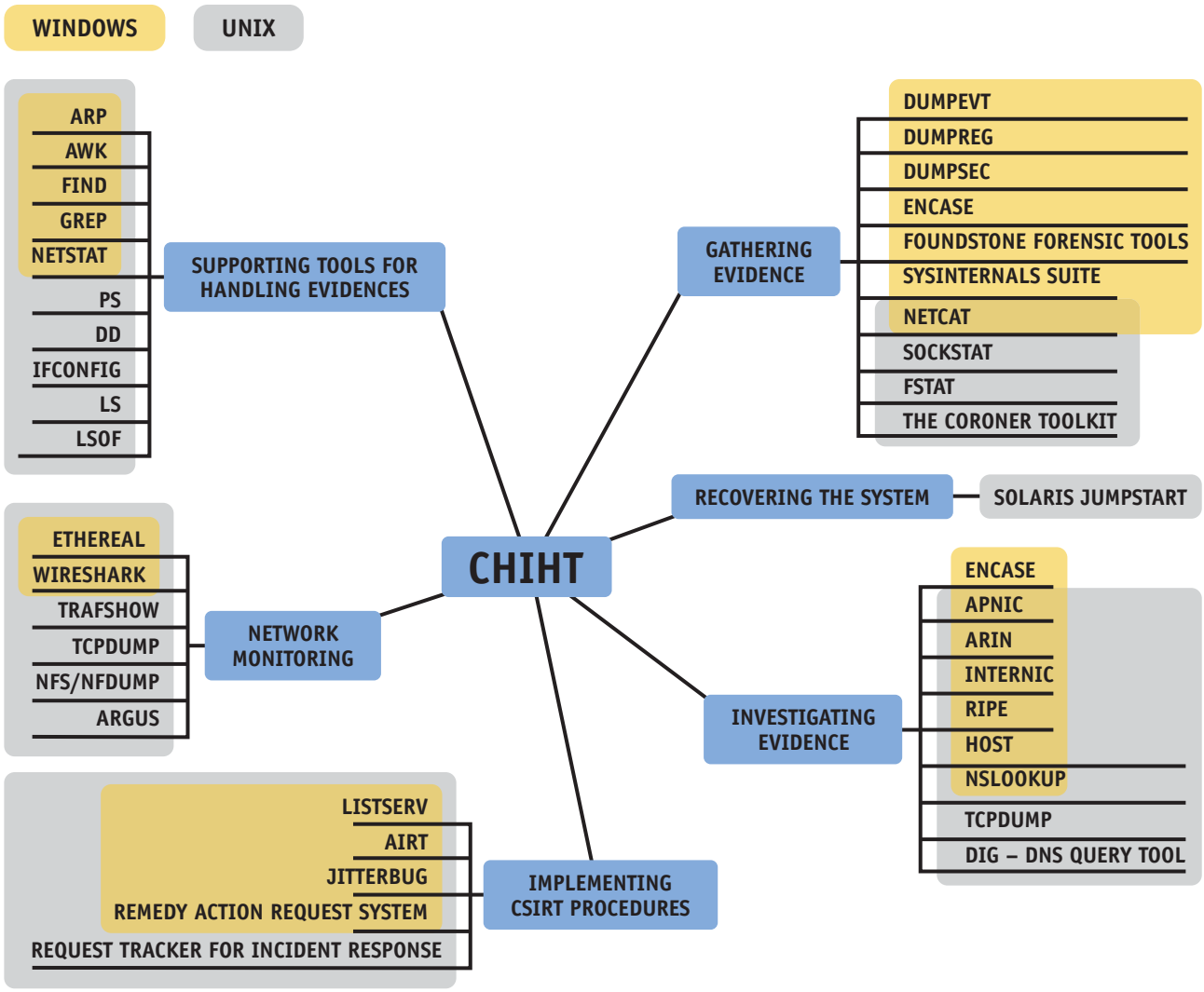


Figure 13 - Clearinghouse for Incident Handling Tools

The mind map above presents all the most important tools in terms of their usefulness in incident handling procedures. They are divided into sections and information (as graphical representation) about operating system availability is provided. As you can see, many of these tools are available for both Windows and UNIX systems. These tools could be used not only by your team but by others as well.

54 CERT Polska website: http://www.cert.pl/

It is a good idea for you to recommend their use to your customers. These tools can increase their IT security level as well as enable them to be ready to help you in detecting new incidents and gathering information about them. This is very good material for your periodic awareness activities.

8.9.2 Incident handling systems

Incident handling systems comprise a special group of tools. In the CHIHT repository you can find three such systems: Application for Incident Response Teams (AIRT), Jitterbug, and Request Tracker for Incident Response (RTIR – the implementation of the Request Tracker ticketing system). The two most popular are AIRT and RTIR.

It is highly recommended that you implement one of these two systems in your infrastructure should you decide to support your workflow[55] with a ticketing system for incidents. They have been specially developed and dedicated for handling security incident tickets and they are used by many teams, so you are likely to easily find support from the CERT community in implementing and using these systems.

Probably, at the moment, the most popular incident handling system is RTIR[56]. RTIR was developed by the RT software owner – Best Practical – with the support of JANET-CERT. Further development of this software was possible thanks to a few other teams which established a working group[57]. Over a few years the group designed and finally developed quite advanced software for CERTs. It has functionality that comes directly from the needs of CERT members so it is highly likely that it also will meet your expectations.

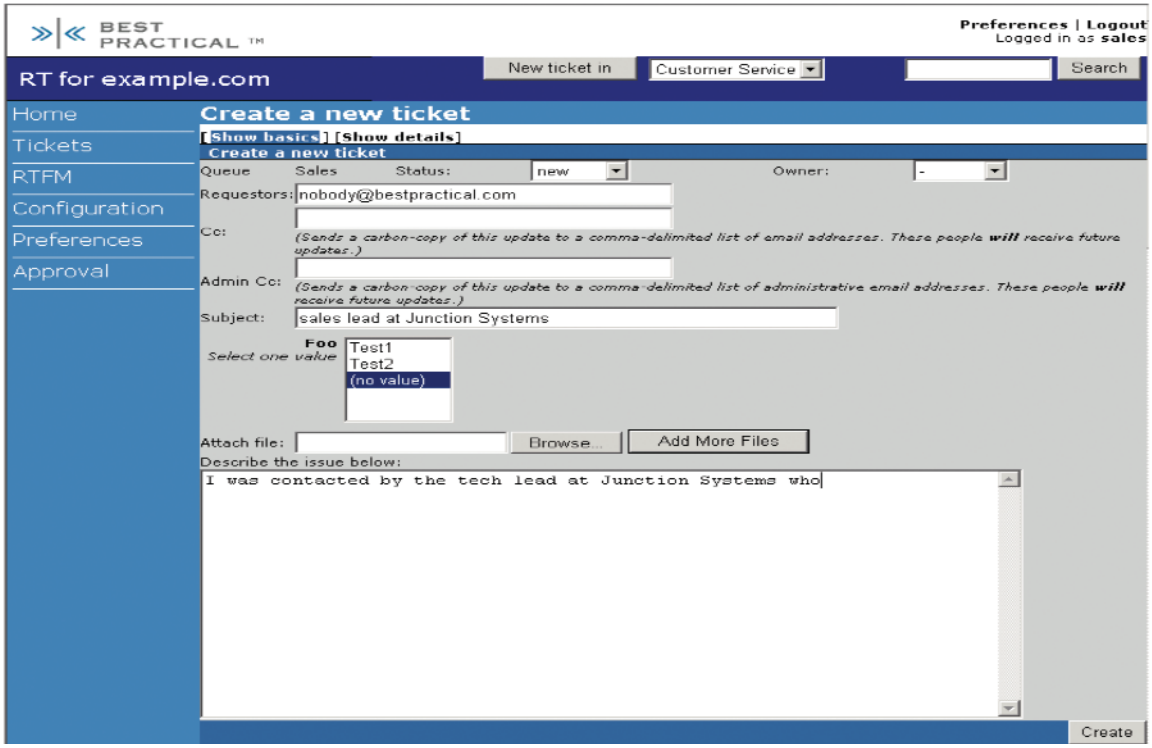


Figure 14 - Request Tracker ticketing system screenshot

55 There is no ready support for a workflow built into these systems but there are some possibilities for adjusting a system to follow your workflow.
56 RT for Incident Response: http://www.bestpractical.com/rtir/index.html
57 Request Tracker for Incident Response Working Group: http://www.terena.org/activities/tf-csirt/rtir.html

8.9.3 Team Cymru 'Who and Why' episodes on security tools

You can find a very helpful set of information about tools in short movies prepared by Team Cymru. They are all available at Team Cymru YouTube channel[58]. At this channel, the following security tools are presented (mostly by interviewing the tools authors):

- SNORT: episode 13[59]
- NMAP: episode 14[60]
- MRTG: episode 15[61]
- NESSUS: episode 16[62]
- SPAMASSASIN: episode 17[63]
- MALWARE HASH REGISTRY: episode 3[64]

8.9.4 Information collection, analysis and publication support tool

GOVCERT.NL has developed a tool called Taranis[65], which has been specifically designed to fit the workflow generally seen in a CERT organization for collecting, analyzing and publishing information. Taranis is based on the workflow consisting of five phases used by GOVCERT.NL:

- Collect: collect information from the sources.
- Assess: determine relevance and discard if necessary.
- Analyze: analyze relevant news-items and determine the appropriate product(s) that are to be created on the subject.
- Write: write the product(s) and apply the standard quality assurance cycle.
- Publish: send out the product(s) to the relevant target audience.

The data that is used in the application is based on internationally accepted standards. Vulnerabilities are directly indicated with Common Vulnerabilities and Exposures (CVE) IDs. The software list is based on the Common Platform Enumeration (CPE) list. Taranis contains mechanisms to keep both lists and the mapping between them up to date.

8.10 Quality assurance

No matter how well you organise 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.

58 The Team Cymru YouTube channel: http://www.youtube.com/teamcymru
59 Episode 13, SNORT: http://www.youtube.com/teamcymru#p/u/61/baxPhu1pA2M
60 Episode 14, NMAP: http://www.youtube.com/teamcymru#p/u/60/8FhDVhVUOS4
61 Episode 15, MRTG: http://www.youtube.com/teamcymru#p/u/59/PwnIbxiIPMQ
62 Episode 16, NESSUS: http://www.youtube.com/teamcymru#p/u/58/EDJziPLM5lU
63 Episode 17, SpamAssassin: http://www.youtube.com/teamcymru#p/u/57/aE6GWwKshiQ
64 Episode 3, WebMHR: http://www.youtube.com/teamcymru#p/u/71/I9d8SeG9t8U
65 All information about Taranis can be found at http://www.govcert.nl/render.html?it=210

8.10.1 How and when to control the process

You can control the incident handling process by observing ongoing activities and you can control it *post factum* when an incident is over. The first method is recommended for critical incidents which you have ranked as the highest according to your methodology for risk assessment[66]. The second method is very good as a regular methodology for process control.

The methods for controlling an incident handling process are similar to any kind of control methodology. You can:

- make daily observations
- analyse documented actions
- interview team members.

Remember that controls, if not properly applied, can produce negative results rather than positive ones. It is recommended that this technique be used reasonably often. One idea is to adjust the frequency to your regular incident handling team meetings. Then a part of this meeting could be dedicated to discussing a particular case and agreeing on its evaluation and possible actions for improvement. So one incident per week to control is good enough, more frequently can be frustrating, and less than one per month is probably not enough. Do not try to control and judge people – focus on processes!

8.10.2 What to control

Generally speaking, your control check list should correspond to the most important rules you have agreed with your team members. Below you can find a proposed checklist form which you can use for control.

Dates of the control	
Controller	
Incident (reference no.)	
Was the procedure followed in handling the incident?	
Were all possible parties involved in the resolution of the incident?	
Did everybody fulfil the tasks according to his or her role in the team?	
Was the incident correctly classified? (compare the classification with other similar incidents)	
Was disclosure policy followed during incident handling? (and was the information exchanged correctly classified)	
Remarks	
Control rank (high / medium / low – score)	
Explanation of the control rank	
Things to improve	

Table 15 – Incident handling process control form

66 To learn more about risk assessment, go to section 8.3 Triage

POLICIES

9 – Policies

Policies lay out principles or rules to guide decisions and achieve rational outcome(s). They are not the same as procedures, which describe in more detail what, how and when to do something within the boundaries of the policy.

Policies need to be clear, easily understandable and capable of being interpreted in only one way. Of course, they should only exist if they have a reason for being, they should be necessary, and they should not overlap with each other. A policy has to be followed up on and people should be able to follow the policies.

Next to creating and using policies, a quality review process should be in place. The feedback on policies is then used and incorporated into the existing policies to make sure these policies are up to date.

9.1 Basic policies

A few policies are basic and independent of the CERTs' services or constituents. These basic policies must always be in place. Important basic policies are:

- information classification policy
- information disclosure policy
- media policy
- privacy policy
- security policy.

In the following paragraphs these policies will be discussed on a high level and in generic terms.

9.1.1 Information classification policy

Classification of information is essential to a CERT. Without classification everyone treats the same piece of information differently, which could have major consequences. Therefore, to get everyone on the same page, a policy is needed.

The information classification policy is closely tied to the security policy and the information disclosure policy, which should describe principles that need to be followed to protect information and how and to whom you can distribute information with a particular classification.

The complexity of the policy depends on the mission, your constituency and whether you are bound by a superior policy within your organisation (eg, government CERTs typically have to follow the same information classification policy as the state government).

A simple scheme would be to differentiate between confidential and public information. A more complex scheme would incorporate, for example, 'internal' or 'personnel confidential' into the classification.

As CERTs communicate with each other using the Traffic Light Protocol, it would be wise to have at least the same four levels of confidentiality: red, amber, green and white[67].

As a CERT depends heavily on receiving and sharing information with others, careful consideration should be given to classification. On the other hand, if too low a classification is assigned, there is the risk of information being leaked and therefore trust being lost within the community or with your constituents.

9.1.2 Information disclosure policy

As mentioned in the last paragraph, sharing information with your constituents and other teams is essential. To do this effectively, trust is needed with and between teams and constituents. Without the ability to share and receive information in a trustworthy manner, the team will not be able to act successfully. A policy is needed that obliges everyone within the team to do this in the same effective and secure way. The policy needs to answer the following questions:

- What pieces information should be disclosed?
- To whom should this information be disclosed?
- When should it be disclosed?
- What is the recipient permitted to do with this information?

9.1.3 Media policy

The news media are pervasive. The moment a serious incident occurs they are onto it and start gathering information from everywhere. Probably they will start asking you questions too. How do you handle these questions? Will you answer all the media, or only the ones you know? Or will you just simply reply: 'no comment'.

To help you organise PR work, you can use advice prepared by CERT/CC[68]. This proposes, amongst other things, the following for media policy and your PR process:

- Define and set expectations.
- Define the process for what needs to be done, including roles and responsibilities.
- Define key messages that need to be conveyed to different audiences based on the nature of the incident.
- Provide names and contact information for media and press contacts.
- Provide names and contact information for experts who may be needed to speak to the media.

THE MEDIA POLICY CASE STUDY

In one case, a CERT read in online media that a small office of a constituent had experienced an incident. The constituent's spokesperson had said it was a minor incident and that they would be up and working within a few hours.

When the CERT contacted its trusted person at the constituent, they learned that it was not a small incident, but rather that many of their offices had been infected, including their head office.

The CERT helped coordinate the response to the incident and, in particular, helped the spokesperson to get the correct information from the incident management team, so he could give the right information to the media.

67 For more information, see section 8.8.1 Traffic Light Protocol
68 *Crisis Communications During a Security Incident*: http://www.cert.org/podcast/notes/13kimberland.html

Such a plan needs to be consistent with and reflect the organisation's communication strategy and objectives.

Interacting with the media may involve:

- establishing solid relationships well in advance of any security event;
- researching the incident that members of the media are asking about;
- contacting reporters (or their editorial desks), news services, newspapers and TV channels, and other media outlets;
- providing organisational contact information for further inquiries.

Public relations challenges during a crisis situation include (note that in organisations where a crisis team is formed in such cases, they will then take over this responsibility):

- coordinating and logging all requests for interviews;
- handling and 'triaging' phone calls and e-mail requests;
- matching media requests with appropriate and available internal experts who are ready to be interviewed;
- making sure that all of information provided to the media is accurate and does not inadvertently escalate the situation.

Important aspects of the policy should include the following considerations:

- Only answer media questions through your spokesperson.
- Do you or your constituent speak to the media about the incident?
  - Offer help to your constituent's spokesperson. He probably does not deal with these incidents on a daily basis.
- If possible, take the time to answer questions with the team and your constituent.
- As a team, always keep your spokesperson well informed, without sharing confidential information.

9.1.4 Privacy policy

Most European countries have a personal data protection and privacy laws which are based on directives by the European Union[69].

Your policy must comply with your national privacy and data protection laws. Make sure that you have written down what is considered personal data, and what you will do with that data to abide by the law. Be aware that some countries have different interpretations as to what constitutes private data.

You should ask yourself the following questions, at least, regarding the processing and storing of personal data:

- Why am I doing this?
- What is the least I could do to achieve this?
- Is doing this proportionate to the risk and benefit involved?
- What legal duties does it involve?

69 Summaries of EU legislation: data protection in the electronic communications sector - http://europa.eu/legislation_summaries/information_society/l24120_en.htm; protection of personal data - http://europa.eu/legislation_summaries/information_society/l14012_en.htm

9.1.5 Security policy

A security policy describes the measures which need to be taken to reduce the most prominent risks. The policy should involve all aspects of security: physical and environmental security, personnel security and IT security.

It is beyond the scope of this guide to list all possible risks for a CERT in this document. You need to make your own risk assessments. However one risk that is imminent for all CERTs is the risk of losing its capability to act on incidents and not being able to interact with other teams anymore. As CERTs try to eliminate intrusions, malware infections, etc, they are also prime targets for miscreants making efforts to undermine the CERT's capabilities and trying to steal confidential information available in that CERT. Miscreants use both IT related attacks and attacks against your personnel or facilities.

The security policy needs to cover all aspects relevant to the team, its IT infrastructure and all connections to the outer world, as well as the team's physical well-being.

- **Physical security**

The security of the building(s) you are working in: what are your requirements for guards, on who has access to the building, on how to cope with guests, the structure of the building, the location of the building, and the security of your IT systems as well as access to those systems?

- **Personnel security**

The security of your personnel: does anyone need to know who is handling incidents in your team? How would you restrict this knowledge? To what extent are your personnel allowed to mention that they work for your team? To what extent can they talk about this in public, in bars, etc? Make sure you give reasons and guidelines on how to cope with questions and on being careful. Be sure to write a procedure for your employees on how to cope with personal threats (see the example in the text box above).

EXAMPLE:

A CERT incident handler was threatened by a miscreant: his family would suffer if he continued to hunt down specific malware distribution sites. The employee had mentioned what work he did and for what organisation on several social networking sites. The CERT immediately stopped doing this work for a period of time. The employee eventually quit the job himself and started working elsewhere.

- **ICT (information and communication technologies) security**

ICT security covers policies on your local network security, computer security, information security, including continuity of operations, and the handling of internal incidents.

9.2 Human resources

As CERT work is, to a large extent, customer focused, a CERT's personnel must be competent and trustworthy and they should be able to communicate effectively with its constituents.

Next to the required technical skills, incident handlers should have sufficient skills in the following 'soft' areas:

- communication skills – being able to effectively communicate with constituents, their own team and their team leader or manager;
- analytical skills – being able to quickly analyse a situation and make appropriate decisions;
- networking skills – being able to quickly gain the confidence of other people and sustain those relationships;
- security skills – being aware of the risks and threats that are out there, and being able to explain those threats to non-IT people in simple terms;
- stress resistant – being able to prioritise, remain calm under high pressure.

To be able to cope with different incidents, your incident handlers should have in-depth knowledge of certain aspects. As no-one can know everything in depth, you should have a diverse team.

EXAMPLE:

In one incident there was an outbreak of a worm. When the team was getting in, the constituent's personnel were cleaning PCs, but the worm kept coming back. The first tasks were to get a copy of the worm, and to monitor the network to see what was going on.

The analysis of the worm together with the network analysis quickly showed how the worm was spreading and the vulnerabilities it exploited to infect PCs. By closing down certain ports to keep the worm from spreading between parts of the network, the worm could slowly be quarantined. To ensure that the worm would not come in through a laptop, for example, a small program was written to alert the system administrators when network traffic was showing symptoms of this worm.

A combination of a malware specialist, a network specialist and a programmer, and the way the coordination of the incident was handled by the team, ensured that the incident could be solved relatively quickly.

SUGGESTION

Your team should include the following hard skills:

- malware analysis
- forensic analysis on different operating systems
- network specialist
- web security specialist
- programmers in various languages such as Perl, Ruby, Bash scripting, C, etc.

To make an all-round team, differences in character are a necessity. Incident handlers need to be creative most of the time, but very precise and orderly people are also needed.

9.2.1 Hiring staff

Getting the right people on board is a difficult task. Next to the necessary technical and social skills, they need to fit in with a CERT. Experience shows that people may be great at their job, but when a high-pressure incident comes around, even when they are not working on that incident, they totally collapse. Therefore it is absolutely necessary to have a good hiring process in place that tests their suitability for every aspect of the work they will be doing. Remember: people can be trained in technical skills, but training them to resist stress is a lot harder.

SUGGESTION

Next to your organisational procedures on hiring new staff, make sure you follow the following steps at least to save yourself a lot of time:

- CV (résumé, short biography) reviewed by at least two persons – before the interview.
- If in doubt as to who to choose for an interview, carry out telephone pre-interview screening
- Have a first interview, preferably with two interviewers. Test relevant skills and experiences as mentioned in the candidate's résumé and try to test their stress resistance. Also assess if the candidate would fit in with the team.
- Have a second interview with the remaining potential candidates. Involve different interviewers if possible.
- Have a third round, in which the candidate presents or is asked how he or she would deal with a specific case.
- Perform the appropriate reference checks with other CERTs, and security clearance checks if appropriate.

Although this is a time-consuming process, it saves time when someone is hired. You have a better chance of getting the right person on board.

Job interview questions could involve the following[70]:

- What is security in your opinion?
- How do you maintain your knowledge on security?
- What is your experience with incidents?
- How did you handle those incidents?
- Give the candidate a case study for comment
- Use stress-inducing questioning (two persons firing different questions)
  - How does he handle various questions; can he finish his story?
  - Does he remember where he was with the last answer?
  - Does he remember the last question?

9.2.2 Staff training

People will never stop learning. People also want to be trained on the job, and use their job to widen and deepen their skills and work on their personal development.

As a CERT, you need to keep investing in your people to widen the skills of your staff in order to foster their personal development and nurture the skills in the team. This will keep the overall skill-set of the CERT up to date with fast developing technologies and trends in attacks.

For incident management the following training could be applicable:

- Transits[71]
- malware analysis
- forensic analysis
- incident management
- communications skills
- analytical skills
- media training (television and written press)
- conferences
- technical skills.

70 To learn more about the recruitment procedure and interview questions, do exercise 3 from the ENISA *CERT Exercises Handbook*: http://www.enisa.europa.eu/act/cert/support/exercise/

71 For more information on TRANSITS training, please visit http://www.terena.org/activities/csirt-training/

As there are still not many training courses explicitly for CERTs, except in the USA with CERT/CC, it is hard to train you employees in CERT specifics. As a result, more and more CERTs are arranging for internships with other CERTs.

9.2.3 Entry and exit procedures

As CERT personnel are hard to get, you should make sure that new people are brought up to speed quickly, and have enough challenges and variety in their jobs to ensure you can retain them. You should also make sure that when they leave, the proper actions are taken.

When a team member leaves, bear in mind that he had access to confidential or sensitive information. It is therefore essential to revoke access to this information as soon as possible and to remind him of his non-disclosure agreement with the team.

There are two ways in which people can leave. They get fired or they quit themselves. Research shows that a substantial percentage[72] of incidents come from (former) internal people. They want revenge, they do not like their boss, they are jealous, etc. Also it happens that employees who leave steal data to leverage a new job. Thus, not only when employees get fired but also when they quit themselves, you need to act quickly to make sure they do not retain access to confidential information anymore.

Exit procedures should always be followed without question. The exit procedures should aim at the following, the moment you know a person is going to leave:

- removing access to systems with confidential information (changing password, revoking certificates and keys, blocking accounts, etc);
- logging the actions of the employee leaving;
- backing up all his work;
- revoking his roles in incident management;
- interviewing to hand over to the next person;
- performing exit-interview to learn for the future;
- announcing staff change to constituents, parent organisation, and other teams.

If a person gets fired, more rigorous measures have to be taken. As well as the procedures mentioned above, the following have to be done immediately:

- revoking access to the building;
- escorting the person out of the building using a security officer or guard;
- removing access to any system.

No matter how much you trust the person who is leaving, always log what he is doing and revoke access to the most sensitive systems.

72 CERT.org has done research on insider threats: http://www.cert.org/insider_threat/

9.3 Code of practice

In many professional environments, where medical professionals, engineers, lawyers and therapists work for example, it is established practice to have rules of conduct for professional behaviour. Sometimes these have a legal background; often they are imposed by membership of a professional society or organisation. The term 'code of practice' is used here to refer to such frameworks.

The CERT community is very young – it has only been in existence since 1989. Practices similar to those just described are slowly coming into existence. You are recommended, however, to draw up such a code of practice for your CERT – and to discuss it with your team members. The CERT community in fact implicitly expects CERT professionals to behave in a responsible way, especially when dealing with information, but also certainly in regard to responsible disclosure.

The European CERT community, more specifically the Trusted Introducer community, has made available a code of practice which they strongly recommend to their members[73]. It is re-printed here as an annex; see 14.2 Annex II - CSIRT Code of Practice.

73 Trusted Introducer documents: https://www.trusted-introducer.org/links/documents.html

NATIONAL AND INTERNATIONAL COOPERATION

10 – National and International Cooperation

Your CERT will need to cooperate with the world outside your constituency and organisation. Complaints or warnings, which your team will need to handle, may come from external parties. Alternatively you may have an incident going on for which the source is outside your constituency, and which you want to stop and preferably have the root cause removed, if possible.

For these reasons, your CERT must cooperate with, for example, other CERTs, abuse teams, internet service providers and also, in special cases, with law enforcement agencies.

Some CERTs have subscribed to the service of an 'upstream' CERT, which undertakes national or international networking for them. For example, this applies to many university CERTs in Europe as they can usually ask their NREN[74] CERT to take care of those activities. In addition, some organisations 'buy' their CERT service or parts of it from a commercial provider – and then they can reasonably expect that this commercial CERT will do this networking on their behalf.

Most CERTs however will need to do their own networking outside their organisation. In the next few sub-sections you will see some of the forms of structure, national, regional, worldwide and sectoral that are present and which have allowed the CERT community worldwide to keep working together effectively, despite the growing number of teams involved.

It is regarded as important that you as a CERT invest in these relationships with other CERTs and security teams. This investment includes joining those arrangements relevant for you – examples you will find below. It also includes going out and meeting people – this is an excellent way to improve your network and will contribute to building relationships of trust with other teams.

You also need to present yourself to other CERTs and the world. Say who you are, what constituency you serve, when and how you can be reached, how you handle confidential reports, etc. The best thing to do is simply fill out RFC-2350 and publish it on your website – that is what this RFC was meant for and it is the only standard of its kind[75]. Also, as urged previously, register an *IRT-object* for your CERT in the RIPE database.

10.1 Bilateral cooperation

It is good practice to assess which security teams or CERTs are important enough to you that you should have a direct bilateral relationship with them. If you have an 'upstream' CERT who delivers services to you – that is an obvious one you need to work with. Also think of the internet service provider of your organisation – get in touch with their security team and their CISO. Does your country have a national or a government CERT? – talk with them. What about the police, do they have a cybercrime unit or something similar? – get to know some of these people.

In general terms – when a bad incident strikes, it is usually too late for you to make the acquaintance of other teams. You will not have time then. So connect with those colleagues when things are relatively quiet. Experience shows this is a good investment of your time.

74 NREN stands for National Research and Education Network – like DFN in Germany, JANET in the UK or GRNET in Greece
75 Expectations for Computer Security Incident Response: http://www.ietf.org/rfc/rfc2350.txt

10.2 National cooperation

In more and more countries, national structures (forums, organisations) for cooperation of CERTs are being established. Examples from Poland, Germany and The Netherlands show that these structures for cooperation are considered very useful by the participants. If your country has a national team or a government CERT – ask them whether the country has a national structure for cooperation and, if so, under what conditions your team may join. If there is no such team yet, consult the NREN in your country – most European countries have a national research network and usually they operate a CERT. If you are in the EU, ask ENISA.

If you are in a position to establish a national structure for cooperation, it is advisable to talk first with colleagues in other countries who have already set one up. They can provide you with the rules for good cooperation, and what can be achieved in such structure of cooperation and what cannot. Structures for national cooperation in general are confidential and not available on the internet. But some national cooperation activities and projects among others are listed on ENISA webpage[76].

To find like-minded colleagues, also use networks, especially those provided by TF-CSIRT and the Trusted Introducer – for both, see the following paragraphs.

10.3 Critical infrastructure protection

If your CERT and constituency also protect assets or networks which can be regarded as 'critical infrastructure' then you are strongly advised to get in touch with your national and/or governmental CERT to discuss this.

The definition of what is critical is widening. Now, besides traditional sectors such as transport, energy, utilities, etc, critical information infrastructures such as internet exchange points, network communication lines and other possible ICT 'choke points' are being focused on by policy-makers[77]. This is happening because many critical services and processes are becoming increasingly dependent on the functioning of ICT networks and electronic communication services. Networks are now vital to citizens, businesses and governments and provide the backbone of the economy.

10.4 Sectoral cooperation

If your organisation or constituency is a member of a 'sector' that has its own forms of cooperation already then make sure you find out whether there is cooperation on IT security issues or, indeed, whether a structures for CERT exist. Join such an effort, if it exists – or pioneer such a form of cooperation yourself.

These forms of cooperation are proving very useful for financial institutions, for example. NRENs are also long-standing examples of fruitful sectoral cooperation.

76 Cooperation activities and projects: http://www.enisa.europa.eu/act/cert/background/inv/cert-activities/co-operation/cooperations
77 CIIP - a new initiative in 2009: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/

When such structures for cooperation are new and especially when the participants come from competing organisations, as is the case with banks for instance, then you will need to invest time and effort in bridging the differences. The fact is that all CERTs share the same goal, whether there is competitiveness in the commercial arena or not; with regards to security violations they have a 'shared enemy'. For this reason, the CERTs of banks or of hardware and software vendors are cooperating successfully, and have been doing so for many years.

10.5 TF-CSIRT

If your CERT is located in Europe or around the Mediterranean Sea and you need to build cooperation with other CERTs outside your own organisation, join the TF-CSIRT mailing list and attend their meetings as often as you see fit[78].

TF-CSIRT emerged in 2000 out of the regular meetings of European CERTs, which had already started in 1993. TF-CSIRT is simply a meeting place for all European CERTs and abuse teams. There is no formal membership or membership fee – but to join you need to be a member of an existing CERT or abuse team, or one that is being built – or at least be able to document a genuine interest in the community, including a willingness to contribute to that community.

TF-CSIRT meets three times a year, all over Europe. To go to some of these meetings is the best guarantee for finding colleagues who share the same challenges that you have – some of whom may have the experience to help you along, as you are expected to help others when you can. This has been the recipe for the success of TF-CSIRT ever since 1993, and it continues to deliver good value to many teams and great value to new ones.

10.6 Trusted Introducer

The 'Trusted Introducer for CERTs in Europe' or TI serves as a 'trusted backbone' of TF-CSIRT. Whereas membership of TF-CSIRT is relatively open (see above), the membership of the TI requires that the CERT in question be accredited by the Trusted Introducer and pays an annual fee[79].

Before a CERT becomes 'accredited' and thus a member of the TI, it is the possible for the team to become 'listed' by the TI. Listing is free of charge and requires two supporters from among the accredited teams. A listed team's contact data are specified on the public TI website, and thus available for the world to see.

'Accreditation' requires not only paying an annual fee but also meeting certain basic requirements. The status as of September 2010 is that the TI has accredited 73 European CERTs. These teams come from all sectors in Europe.

The accredited teams meet three times per year, adjacent to TF-CSIRT meetings. These meetings are closed. They are excellent opportunities to meet your CERT colleagues and discuss potentially confidential issues.

In September 2010, the TI community added 'certification' as an extra option for an accredited team. To become 'certified', the team needs to meet additional and stronger requirements, which are measured against a CERT maturity model.

78 You will find all TF-CSIRT information at: http://www.terena.org/activities/tf-csirt/
79 You will find all TI related information at: https://www.trusted-introducer.org/

10.7 ENISA

ENISA, the European Network and Information Security Agency, provides, among many other activities related to IT security in the European Union, reference materials, good practice guides and exercise material for CERTs. ENISA also regularly supports CERT training activities in Europe, such as TRANSITS[80].

10.8 European Government CERTs (EGC) group[81]

The EGC group is an informal group of governmental CSIRTs that is developing effective co-operation between its members on matters relating to incident response, by building upon the similarity in constituencies and problem-sets between governmental CSIRTs in Europe.

To achieve this goal, EGC group members will:

- jointly develop measures to deal with large-scale or regional network security incidents;
- facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities;
- identify areas of specialist knowledge and expertise that could be shared within the group;
- identify areas of collaborative research and development on subjects of mutual interest;
- encourage the formation of government CSIRTs in European countries;
- communicate common views with other initiatives and organizations.

10.9 FIRST

FIRST, the Forum of Incident Response and Security Teams, is the global meeting place for CERTs, and has been since its inception in 1990. FIRST's most popular service is their annual conference. In addition, FIRST organises workshops and supports special interest groups. Since 2007, FIRST and the TF-CSIRT have been organising one joint meeting or workshop each year.

If you cooperate not only in Europe but also in the global environment, it is recommended that you consider becoming a FIRST member, which requires an annual fee[82].

80 You will find all CERT-related ENISA information at: http://www.enisa.europa.eu/act/cert/
81 All EGC information can be found at http://www.egc-group.org/
82 You will find all FIRST related information at: http://www.first.org/

OUTSOURCING

11 – Outsourcing

This chapter will discuss the outsourcing of incident management from the CERT point of view. It will not discuss outsourcing the CERT in part or whole from the point of view of a hosting organisation.

Incident management is the core business of a CERT. For businesses, outsourcing is usually a way to cut costs but most of all to regain maximum focus on their core processes. Therefore it is strange to talk about outsourcing incident management as this is a CERT's core business. Therefore we will not talk about outsourcing all of your incident management but, in this section, provide options on which parts of your incident management process you could outsource and under what conditions. Also we will advise on what you should not outsource.

At this time we have not found any national or governmental CERT that actually outsourced any part of their incident management process. They either just do not deliver a particular service or they deliver it themselves.

We do know however that there are CERTs that have outsourced some part of their incident management process. So, for the practical guidance that we cannot gain from national or government CERTs, we will rely on other organisational CERTs, the best of our own knowledge and our general experience in IT outsourcing, IT security and other outsourcing.

We are also seeing some movement in this area. Although technically it is not formally outsourcing, there are national and governmental CERTs that talk about cooperating with each other; eg, where a certain CERT will deliver services to another CERT which does not have the required capabilities. This is still at a very early stage but is, nevertheless, a way to move forward as not many resources are available in this area.

We will only talk about outsourcing to a third-party such as a managed service provider (MSP). So cooperation, in- or co-sourcing, splitting up your CERT within your organisation, etc, are not part of this guide.

Last but not least, outsourcing is a challenging project, which should not be underestimated. If you do not have the experience, make sure you hire the right people who can guide you in this process.

11.1 What you probably should not outsource

As you are the CERT of your organisation, government or country, you are the one to help in solving an incident.

To be able to discharge this responsibility you need to have control over the incident handling services. Therefore, it is not recommended that you outsource those parts of incident handling that give you that control, such as:

- Incident reports, registration, triage (including verification and classification)
  The CERT is the single point of contact for IT security related incidents. Accepting the report and deciding what to do with the incident is a CERT's responsibility.

- Overall coordination of incident resolution
  To have control also means that you should undertake the high-level coordination of incident resolution activities. Detailed coordination, eg, on site coordination of system repair and recovery, as well as other activities in incident resolution, can be performed by others.

The other core services and extended services mentioned previously in Table 7 can, in principle, all be outsourced.

11.2 Why would you want to outsource part(s) of your incident management process?

For a CERT there are several reasons for outsourcing incident management related services. These reasons could also apply to other organisations, but the main difference is that most of the time a regular business will not outsource their core business. Among those reasons are:

- lack or cost of qualified personnel
- specific expertise needed
- in-depth expertise needed
- service needed by your constituents that you do not want to deliver yourself.

EXAMPLES OF OUTSOURCING

EXAMPLE 1
A CERT has outsourced their on-site incident management. The outsourcing partner acts as part of the CERT. During an incident they go on-site and do the analysis of the network, PCs and malware; they meet with local IT staff and management and coordinate the incident on-site together with the constituent.

EXAMPLE 2
A CERT has outsourced only the forensic and malware analysis, and cooperates on the analysis of incident impact. When a constituent is infected, infected hardware is picked up and analysed by the MSP. All results are reported to the CERT, who fully coordinates the incident. Impact analysis is also done in cooperation between the MSP and the CERT. In the case of a criminal act, all evidence can be handed over to the police.

11.3 How to outsource

First of all, it is very important to know the services you want and need to deliver to your constituents. Out of those services a decision has to be made on which of these services you need or want to outsource.

It goes beyond the scope of this guide to describe how you should acquire an MSP, but it is of the utmost importance to at least consider the following rules for outsourcing:

- Why do you need or want to outsource certain services?
- What result do you expect those services to deliver?
- Contract and underlying service level agreement (SLA)
  What reasons or causes will lead to termination of the contract? Think about security errors, incidents, and be specific and detailed. As this is your core business, failure by the MSP will be your failure as a CERT.
- Contract management, both operational and financial
  Often the operational side of controlling your MSP is forgotten. Financially it is managed by a CFO, but whether they deliver what you have agreed upon is not controlled.

- Trustworthiness
  Can your MSP be trusted? Do they have references?
- Security requirements
  Is the MSP able to fulfil the security requirements applicable in your organisation?
- Audit
  Are they audited? Which standards are they audited on? Which standards do you want them to be audited on? Can you require them to be independently audited?
- Security clearance
  Do you need people to have a security clearance if they perform incident management work for you?

As mentioned in the introduction of this section, outsourcing is probably not your everyday task. Make sure you get the right people onboard to help you manage this daunting task. Both in preparation, as in its day-to-day business, outsourcing is quite a task. However, done well, it will give you what you pay for.

PRESENTATIONS TO MANAGEMENT

12 – Presentations to Management

12.1 What information management needs and how often?

Good contact and communication with your management (which is usually an organisation's top management in the case of CERTs) is a very strategic issue and you should not neglect it. Management not only just like to be informed, they really should be informed. Good reporting will help you to save your time and resources in all those situations when you need its operational or financial support and a quick decision.

To make sure you are reporting what your management needs, discuss the issue with your management. It is also very important to think about what you may want and need to report in the future, as in most cases you need to start collecting this data from the beginning.

So, what to report to them:

- What are your operating costs? Are they enough for you to provide your services smoothly and even to develop them?
- Information about the results of your daily operations, for example:
  - number of incidents
  - alarms and warnings issued
  - training and advice provided.
- What are the positive results of your work? What will you maintain and what you would like to change and what do you need to achieve this? For example:
  - average incident resolution time decreased
  - number of infected machines decreased
  - number of advice notices issued increased
  - number of alerts and warnings increased
  - costs of incidents decreased[83].
- Are there any issues which can affect your organisation in the future (in urgent cases report them immediately)?
- What are your plans for the next reporting period in terms of:
  - improving your services
  - recruitment needs
  - tools and devices needed
  - any other investments in time and money.
- What are the most significant risks for your team?
  - financial
  - organisational
  - human resources.

It is good practice to report not only problems but also your proposals for resolving them. Doing this will speed up decision-making and your preferred solution will be implemented.

83 For examples of the costs of incidents, see the second ICAMP report from 2000: http://www.cic.net/Libraries/Technology/ICAMPReport2.sflb

Good reporting practice means that you do not have to do it very often. A quarterly report should be sufficient. Some issues related to investments, recruitment and strategic plans for changes can be reported yearly, together with your yearly report. Of course sudden, unexpected events may need to be reported immediately.

SUGGESTION

'What do incidents cost' is a recurring question. In fact, not much research has been published in this field. This is really a subtopic of quantitative risk analysis. Not an easy task – for instance, how do you value 'loss of reputation'? Also, the number of man-days spent solving an incident are often not accounted for separately and are seen as part of business overhead. However, the 'Incident Cost and Modelling Project' (ICAMP) produced two reports in this area, one in 1998 and an updated version in 2000, that make interesting reading[84].

12.2 How to present a report

The statement that senior managers have no time is a truism, but it bears repeating. You could provide them with a comprehensive and detailed report but it is unlikely they would read it. There are three basic rules for effective communication with senior management:

- prepare a 1-2 page summary
- highlight the most important issues
- illustrate whatever you can.

SUGGESTION

Finally, once you have a report ready, arrange even a short meeting with your management to present it. Do not assume that management will read your report carefully before this meeting. It is better to assume that the person to whom you are presenting it will be seeing it for the first time.

REPORT FOR MANAGEMENT

- SHORT EXECUTIVE SUMMARY (1-2 PAGES)
- THE MOST IMPORTANT ISSUES (NO MORE THAN 10 POINTS)
- GRAPHICAL REPRESENTATION (1-3 FIGURES, STATISTICS)
- FULL REPORT AS AN ATTACHMENT

REGULAR FULL REPORT

- COMPREHENSIVE DESCRIPTION OF ALL ISSUES
- ALL ACTIONS AND PROPOSALS DESCRIBED IN DETAIL
- MANY FIGURES, TABLES AND OTHER GRAPHICS

Figure 15 - Regular full report versus specific report for management

84 Both reports can be found on http://www.cic.net/Home/Reports.aspx: click on the '+' before 'Technology' and you will directly see the ICAMP links. The direct links are: http://www.cic.net/Libraries/Technology/ICAMPReport1.sflb for the 1998, and http://www.cic.net/Libraries/Technology/ICAMPReport2.sflb for the 2000 report.

REFERENCES

13 – References

13.1 How to use: *Step-by-Step approach on how to setup a CSIRT*

This document[85] describes the process of setting up a CSIRT from all relevant perspectives such as business management, process management and the technical perspective. It was published in 2006. It is very useful material for anyone who decides to set up a CERT. It contains 12 chapters, and in it you will find general strategies such as 'planning and setting up a CERT' as well as concrete examples of procedures and ideas – eg, chapter 8 – Examples of operational and technical procedures. From the incident handling point of view the most interesting chapter is chapter 8. In this chapter you will find information on how to:

- collect information about technical components in your constituency;
- identify the authenticity of a message and its source;
- asses the severity of an incident by implementing a simple method for risk analysis;
- organise your work of incident receiving, incident evaluation and incident resolution.

The rest of the chapters relate to the other incident services and rules. It is a very good idea to go through the guide and treat it as a checklist. Even if you already have an experienced and fully established CERT, you will find many good ideas on how to improve your services.

13.2 How to use: *CERT Exercises Handbook*

In this guide there are a number of suggestions on the use of particular exercises from the *CERT Exercises Handbook*[86]. You should follow these suggestions and go to a particular exercise when it is suggested. Each exercise provides you with information about its objective, the targeted audience, the total duration, the detailed time schedule, and the frequency. The detailed courses of the exercises are also provided and you can follow them to successfully conduct the exercises. At the end of each exercise, you can find evaluation metrics which will help you to carry out self-evaluation.

If you want to learn more on how to conduct these exercises (especially exercises 7 and 9) read *A field report from the pilot*[87]. You can find many tips and much advice in this document. Some of these are universal and may be applied to all exercises.

Generally speaking, from the incident handling point of view, the following exercises are the most helpful and valuable[88]:

85 *A step-by-step approach on how to set up a CSIRT*: http://www.enisa.europa.eu/act/cert/support/guide
86 ENISA exercise material home page: http://www.enisa.europa.eu/act/cert/support/exercise
87 Field report on pilots: http://www.enisa.europa.eu/act/cert/support/exercise/files/field-report-pilots
88 Short description from the book included

- Exercise 1: Triage and Basic Incident Handling

This exercise provides students with experience of real-life incident reports, their ambiguity and complexity. After finishing the exercise they should understand what to focus on during initial analysis, how different factors may affect priorities and how to communicate with reporters as well as third-parties. During the exercise, they will apply a given classification scheme to incidents – the purpose of this part of the exercise is to work on the consistent classification of disputable cases (eg, worm v scanning) across team members and possibly to suggest a clearer, more unambiguous classification scheme for the team.

- Exercise 2: Incident Handling Procedure Testing

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 organise this process in their teams in the most efficient way.

- Exercise 7: Network Forensics

The objective of the exercise is to familiarise students with standard network monitoring tools, their output and applications for the analysis of network security events. As a result, students will be able to interpret the security context of collected network data, thus enabling the post-mortem analysis of security incidents.

- Exercise 8: Establishing External Contacts

This exercise is primarily targeted at new and future employees of CERTs. It requires an understanding of internet attacks and communication skills. The students should also be good in written and spoken English.

- Exercise 9: Large-scale Incident Handling

The main objective of the exercise is to teach incident handlers the key information and actions required for the successful resolution of large-scale incidents.

- Exercise 10: Automation in Incident Handling

The purpose of this exercise is to develop students' abilities to create custom scripts and filters dealing with large amounts of data such as IP addresses. After completing the exercise students should be able to extract useful information from bulk data, even in non-standard formats.

- Exercise 11: Incident Handling in Live Role-playing

The exercise simulates a real-life incident, involving many parties with conflicts of interests, different mindsets and legal frameworks, etc. With the introduction of such aspects as vulnerability handling, responsible disclosure and company security management, it helps the students to understand why incident handling is, in many cases, a complex task and what kinds of technical and social skills are required for this job.

13.3 How to use: 'Clearing House for Incident Handling Tools'

Clearing House for Incident Handling Tools (CHIHT) is the repository of many useful tools and guidelines which help you to organise and improve practically all CERT services[89]. You can find the tools which are the most valuable for your incident handling process and how to use them in section 8.9 Tools.

13.4 *How to use: Handbook for Computer Security Incident Response Teams (CSIRTs)*[90]

This document was written in 1998 by Klaus-Peter Kossakowski, Don Stikvoort and Moira West-Brown and updated in 2003 to provide a resource for both newly-forming teams and existing teams whose services, policies, and procedures are not clearly defined or documented. Ideally this document should be used at the stage when an organisation has obtained management support and funding to form a CERT, prior to the team becoming operational. However, the material is still of use to operational teams too.

This handbook can be used by a newly-forming team as the basis for understanding the issues involved in establishing a CSIRT. The information can then be used to assist the development of detailed domain- or organisation-specific service definitions, policies, procedures and operational issues. As a result of applying the material provided in this document, an organisation should be on a fast track to a documented, reliable, effective and responsible incident response service. An existing team can use this document to ensure that they have covered the main issues and options that they consider appropriate for their organisation when developing their incident response service.

89 Clearinghouse for Incident Handling Tools: http://www.enisa.europa.eu/act/cert/support/chiht
90 *Handbook for Computer Security Incident Response Teams (CSIRTs)*: http://www.cert.org/archive/pdf/csirt-handbook.pdf

ANNEXES

14 – Annexes

14.1 Annex I – CERT extended services

Apart from the set of basic services[91] there are other services which can be delivered by a CERT team, the 'extended services'. Some of these you can find described below. Typically these are found in the lists of services of existing CERTs. You can use these to consider how you can improve your relationship with your constituency and your understanding of the simple practical ideas behind them.

14.1.1 Forensics

The forensics service covers both computer and network forensics. Both are very practical and can significantly improve your service-delivery. In almost all cases which will be reported to your team, you can use forensics as a supporting service – especially network forensics because computer forensics is typically much more expensive to conduct for your operation. Usually you are not able to perform computer forensics analysis on the attack target's computer easily. It is simply out of your control and remote analysis is hard and time consuming without any guarantee of success.

It is good practice to focus on and develop network monitoring capabilities. Find the optimal place for network monitoring in your network and set up a network monitoring system[92]. It could be one of many available commercial solutions or your own proprietary system which corresponds to your needs. A simple set of shell scripts together with an effective collecting system for network logs is very often more than adequate. Use the network monitoring system to:

- confirm or exclude reported incidents;
- find more data related to reported incidents;
- establish a filter to discover interesting kinds of attack or particular attacks on your constituency.

You can find more interesting ideas and best practices related to the network monitoring service by exploring the results of the work of FIRST Network Monitoring Special Interest Group[93].

14.1.2 Vulnerability handling

Vulnerability handling is another important service which could be delivered by a CERT team. This service is very much dependant on the positive answer to the question: 'Is any vendor part of your constituency?' Perhaps you are a CERT within a vendor organisational structure. For most teams this is not the case. However it does not mean that in other constituencies there is nothing to do in regards to vulnerability handling services. If, within your constituency, there are significant players such as a dominant TELECOM internet provider, large content providing services or other services which are simply widely recognised and used by internet users, you can provide a service very similar to the classic vulnerability handling service provided by vendors.

---

91 According to *A step-by-step approach on how to set up a CSIRT*, http://www.enisa.europa.eu/act/cert/support/guide, the basic CERT services are incident handling, alerts and warnings, and announcements.
92 When setting up a network monitoring system, keep in mind applicable data protection legislation, eg, the EU Directive on privacy and electronic communications: http://europa.eu/legislation_summaries/information_society/l24120_en.htm
93 See FIRST Network Monitoring Special Interest Group website: http://www.first.org/global/sigs/monitoring/

If you want to take on the role of a vulnerability handler, you have to be aware that there is no commonly recognised standard for this activity. There are mixed opinions on how and when to disclose information relating to a vulnerability and how to cooperate with 'the problem owner' to reach the best solution, especially with internet users. Opinions vary from very extreme full-disclosure rules to very informal rules in the point of view of the vendor or bug-owner.

When deciding how to deal with this problem, you should not ignore the experience of what is probably the most advanced team in the world (concerning vulnerability handling) – the CERT Coordination Center[94].

The simple guidelines given there should help you to establish your vulnerability handling policy.

14.2 Annex II - CSIRT Code of Practice

This is a reprint of the CCoP document by courtesy of the Trusted Introducer for CERTs in Europe[95].

CCoP - CSIRT Code of Practice – approved version 2.1

v2.1/ Approved Version 15 September 2005

Andrew Cormack
Miroslaw Maj
Dave Parker
Don Stikvoort

NOTE:
This version 2.1 is an approved instance of 'work in progress'. More CSIRT service areas may be covered in later versions. It is however approved and useable in its current form – though not claiming completeness.

This document is set up as a Code of Practice for CSIRTs in general.

94 To find out their views and proposals on rules, check their website: http://www.cert.org/kb/vul_disclosure.html
95 TI Working Documents: https://www.trusted-introducer.org/links/documents.html.

CASE STUDY: PROVIDING A SERVICE OTHER THAN A PRODUCT-ORIENTED VULNERABILITY HANDLING SERVICE

Once an internet user called a CERT to report a specific vulnerability. The report was about a misconfiguration in widely used ADSL modems in the public network of the country's national TELECOM provider (about 90% share of the internet users market). The misconfiguration allowed an attacker to automatically access the modem and change the configuration in such a way that a user would lose his connection to the Internet.

The anonymous incident reporter said that he had talked to the TELECOM but they had not come to an agreement and had not found a solution for this problem. The incident reporter wanted to get recognition for revealing the configuration of the bug or at least a written acknowledgment from the TELECOM board of directors for finding and helping in the resolution of the problem.

The TELECOM representative (TELECOM incident response leader) would not agree to do that. The situation was at a stalemate. The TELECOM even began to threaten the incident reporter. He did not want to back down. The CERT coordinator acted as a mediator but he was not able to achieve success.

Finally, after a phone discussion with the vulnerability reporter, the CERT coordinator came up with the idea of establishing a teleconference between the incident reporter, the TELECOM IRT leader and himself. He did so. After about a 5-minute discussion, the incident reporter and the TELECOM IRT leader found a solution and came to an agreement. The CERT coordinator was virtually silent during most of the discussion. It was enough for both parties that they were aware of his presence. The incident reporter revealed the misconfiguration details and he received an e-mail acknowledgment from the TELECOM IRT leader.

This CCoP was adopted by the TI Accredited Teams at their Lisbon meeting on 15 September 2005, as a SHOULD criterium for accreditation. A SHOULD criterium is highly recommended to follow, but not obligatory. Every team specifies whether they chose to comply, or not – and they can change this choice along the way.

If and when an accredited team complies with this CCoP, then they acknowledge that they have read and understood this document and that their teams will comply with the MUST principles that are stated within it, and give proper attention to the SHOULD principles.

0. Definitions

0.1 'the team': the subject CSIRT evaluating this Code of Practice is referred to as 'the team' below

0.2 'incident' should be read below as 'computer/network security incident'

0.3 'Incident Management' is used below to identify the general CSIRT process, including all possible included or related services, ranging from pro-active auditing to repression – on purpose the terms 'security management' and 'risk management' are avoided since these are generalisations beyond the typical CSIRT scope

0.4 MUST below means: an absolute requirement – note that in some cases the MUST statement is conditioned by elements in the requirement

0.5 SHOULD below means: a strong recommendation, but not a MUST

1. Legal Requirements

1.1 *MUST* The team and its members are expected to comply with the legal requirements of their individual countries at all times whilst dealing with Incident Management matters. [Where there is any conflict, this article always takes precedence over other principles stated in this document.]

1.2 *SHOULD* The team and its members will, to the best of their abilities, take into consideration the legal requirements of other countries when their activities have a cross-border component.

1.3 *SHOULD* In the event that requirement 1.1 leads to a conflict in itself as a result of contradicting legislation applicable to a specific event, the team will give precendence to those parts of the legislation that best reflect the team's professional assessment of how the matter at hand should be resolved.

2. The Team

2.1 *MUST* The team will, considering its own operational requirements, alert those sufficiently trusted peer CSIRTs, Vendors and organisations whose operations, or whose constituencies, are likely to be significantly affected by an event or omission known to the team.

2.2 *SHOULD* The team will in its operations act in such a way that it sets an example of responsible Internet and security behaviour

3. Team Members

3.1 *MUST* The team will ensure that all of its members receive a paper and electronic copy of this document, and will ensure that they have read and understood it.

3.2 *SHOULD* The team will on a regular basis engage its members in discussions on the issues touched by this document – this to help ensure that the team members appreciate the issues at hand and are equipped to act accordingly.

4. Information Handling

4.1 *MUST* The team receiving or holding information, regardless of the subject matter, that may affect either another CSIRT team's constituency, the community of CSIRTs as a whole, or indeed the security of the Internet or users thereof, will handle this information responsibly and protect it against inadvertent disclosure to unauthorised parties.

4.2 *MUST* The team holding information valuable to other CSIRTs or Vendor Teams will give ample consideration to disclosing the information to the appropriate party, at the earliest opportunity, taking into consideration their own organisational responsibilities and security requirements. Third party requirements, e.g. those of Vendors, for any disclosure or non-disclosure of the information will be acknowledged.

4.3 *MUST* As a general rule, any disclosure of information to other CSIRTs, Vendor Teams or other organisations, is done on a need-to-know basis, while protecting stakeholders in an incident as much as possible without turning the incident information into void information, not useable for Incident Handling by the receiving party.

4.4 *MUST* The security of the methods of storing and transmitting information inside or outside the team, will be appropriate to its sensitivity. In general this means that sensitive information will be kept and sent only in encrypted formats or over secure channels – this explicitly includes back-ups of sensitive information.

5. Service specific requirements

The below requirements only are applicable when the team offers the service involved.

5.1 Incident Handling

5.1.1 *MUST* Articles 2.1 and 4.* apply.

5.2 Vulnerability Handling

5.2.1a *MUST* The team actively involved in vulnerability research and disclosure processes will have documented procedures for the proper processing of such research and its results.

5.2.1b *SHOULD* Where appropriate, such procedures will be available for review both by Vendors, trusted peer CSIRTs, or – when appropriate – the CSIRT community as a whole.

5.2.2 *MUST* When the team becomes aware of a particular IT related vulnerability, from whatever source, the information will be handled as defined above under 'Information Handling' and in accordance with the process documented under 5.2.1, throughout the entire research and disclosure process.

5.2.3 *MUST* Where appropriate, and considering the team's own security requirements, the details of the vulnerability and any associated research will be provided to the relevant vendor(s) for assessment and remediation at the earliest opportunity.

5.2.4 *SHOULD* The vendor(s) will be given every reasonable opportunity, consistent with the CSIRT's defined procedures, to complete their remediation processes relating to the vulnerability before any public disclosure by the team.

INDEX-1: FIGURES • INDEX-2: TABLES

15 – Index-1: Figures

16 – Index-2: Tables

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu