EUROPEAN UNION AGENCY
FOR CYBERSECURITY

COOPERATION ACROSS CSIRTS, LE AND THE JUDICIARY

Handbook, Document for trainers

DECEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

CONTACT

For contacting the authors please use CSIRT-LE-cooperation@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Alexandra Michota (ENISA), Andreas Mitrakas (ENISA), Constantinos Patsakis, Václav Stupka

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-332-2, DOI: 10.2824/27536

TABLE OF CONTENTS

1. INTRODUCTION

1.1 THEMATIC AREA

In 2018, ENISA confirmed that Computer Security Incident Response Teams (CSIRTs), Law Enforcement (LE) and the judiciary have complementary roles and structures and that incident handling varies across Member States. The data CSIRTs and Law Enforcement Agencies (LEAs) have access to vary, and affect information sharing between them when they seek to respond to cybercrime. CSIRTs interact frequently with LEAs rather than with the prosecutor. CSIRTs offer support to LEAs to collect and analyse different types of evidence. CSIRTs are called rarely as witnesses in courts but the material they collect during the incident handling might be used to decide on cybercrime cases.

Cooperation challenges are identified in the areas of data retention, sharing of personal data (including IP addresses) and confidentiality of criminal investigations as well as admissibility of digital evidence. Legal challenges are followed by cultural, technical and organisational ones.

Figure 1: ENISA training on CSIRT-LE cooperation - Syllabus

ENISA Training on CSIRT-LE Cooperation - Syllabus	
Keywords:	Computer Security Incident Response Teams (CSIRTS), Law Enforcement (LE), Law Enforcement Agencies (LEAs), Judiciary, Cybercrime, Cooperation, Interaction, Information sharing, Tools, Legal framework, Policy framework, Joint training
Background:	This module is intended to provide trainees with an understanding of the key concepts of knowledge of interactions across the three communities, the fundamental legal and policy requirements, the consequences of not complying with applicable laws and regulations, the responsibilities in relation to the sharing information (segregation or separation of duties - SoD matrices), the best practices on how to enhance this cooperation. Trainees further acquire a better understanding of the tools and methods used for the cooperation between CSIRTs and LE and their interaction with the judiciary aiming to investigate complex criminal structures.
Method of teaching and learning:	• Class lectures, interactive learning (class discussions, group work) and practical problems solved in class. • Case studies are assigned to the trainees and are reviewed in class.
Recommended material:	• ENISA reports • ENISA presentations • Trainer's notes based on recommended material and sources

- **Learning outcomes**

As a result of attending this course, the trainee should be able to:

- Demonstrate knowledge of interactions across the three communities; strengths, needs and limitations
- Analyse the legal and policy framework shaping this cooperation

- Better understand tools and methods used for the cooperation between CSIRTs and LE and their interaction with the judiciary

Target audience

The intended target audience are CSIRTs (mainly national and governmental CSIRTs but not limited to them), LE, prosecutors, judges, as well as individuals and organisations with an interest in Cybersecurity.

Course duration

4 hours

Frequency

At least yearly

2. GENERAL DESCRIPTION

2.1 IMPORTANCE OF COOPERATION AMONG CSIRTs, LE AND THE JUDICIARY

Criminal investigations, as part of the criminal proceedings, are aiming to ascertain whether a crime has been committed and if so, determine its author and the relevant charges. The principles and rules governing criminal proceedings are different from those governing civil, administrative, disciplinary or other proceedings and vary among each state and jurisdiction. Nevertheless, collecting and presenting sufficient evidence related to the criminal charge is an essential element in every formal criminal trial and judicial system (adversarial or non-adversarial). The evidence collected and presented by the prosecution authorities must prove beyond reasonable doubt the crime and its author. Based on these, the judges and/or juries will determine the guilt and the charges on the defendant. It should be noted that evidence varies from physical evidence and testimonies to documents and e-evidence, as is mainly the case when investigating a cybercrime.

During the course of a criminal investigation pertaining to a cybercrime, CSIRTs are requested to interact with LEAs and with members of the judiciary, i.e. prosecutors and judges. Although there is an increased reciprocal understanding of their respective needs among the three communities, CSIRTs, LE and the judiciary have different mandates and objectives as well as different operating policies when collecting, processing and further using information.

The CSIRT community has materially different duties and objectives from the LE community, depending as well on the type of each CSIRT community (governmental, national, sectoral, etc.) and LEA (regional, national, federal, international, etc.). However, when dealing with a potential cybersecurity incident/cybercrime, each community should consider the outreach to other actors that could be involved, keeping in mind the multiple ways of cooperation and the importance of receiving reciprocal feedback on a case. Additional stakeholders may be approached in this cooperation process, such as the judiciary, service operators and service providers, intelligence services, military and international agencies.

CSIRTs do not have the powers of LE and respectively, LE does not have access to intelligence and expertise held by CSIRTs. It is therefore important for these communities to cooperate. However, technical, legal, organisational and cultural challenges can render this cooperation complicated. In addition, those challenges are dealt with differently in each country. A comparison of these different approaches is rather valuable when examining this cooperation. The studies developed by ENISA provide valuable insight into the current state of cooperation and recommendations on how to improve it. (ENISA, 2019)

Both formal and informal procedures may be followed in this cooperation process with the purpose of achieving each community's objective of mitigating incidents and prosecuting crimes, depending also on each community's hierarchical or flat structure, the classification level and the sophistication of the exchanged information. Formal procedure may have the form of an official written request for information regarding a specific case, while informal could have the form of information shared orally during an informal phone call. This cooperation channel may be direct or supported through appointed liaison officers, whose role sometimes has been pointed out as a very important one.

Taking into consideration that cybersecurity incidents do not always correspond to cybercrimes, cooperation between these entities does not take place in all cases.

- Cybercrime: "crimes having a computer as a target and crimes where computer is a tool to commit traditional or new crimes".
- Cybersecurity incident: "any event having an actual adverse effect on the security of network and information system".

Cybercrimes sometimes indeed relate to cybersecurity incidents. Nonetheless, in other cases cybercrimes occur which are not related to cybersecurity incidents or which eventually are not reported.

Throughout this cooperation, CSIRTs, LE and the representatives of the judiciary face multi-layered challenges which can be categorized as legal, organizational, technical and even cultural. Understanding those challenges and thus tackling them is an essential step in order to further enhance the cooperation of these communities and improve their efficiency in fighting against cybercrime threats.

The key areas of improvement regarding the cooperation of these communities are identified as follows:

- The understanding of whether the CSIRTs have to report to/inform LE and/or the judiciary of suspicious criminal activities.
- The knowledge that CSIRTs, LE and the judiciary have on the legal framework concerning their cooperation and interaction.

2.2 LEGAL FRAMEWORK AND INFORMATION FLOW

This part presents an overview of the relevant legal and policy framework that shapes the cooperation and interaction between CSIRTs, LE and their interaction with the judiciary in the context of fighting against cybercrime by identifying the information flow pattern among these key stakeholders.

2.2.1 Legal Framework of CSIRT, LE and Judiciary Cooperation

The legal and policy framework that governs and shapes the cooperation between CSIRTs and LE and their interaction with the judiciary in the context of fighting against cybercrime is categorised in three levels:

- **National level:** The national legal and policy framework governs and shapes the cooperation between CSIRTs and LE and their interaction with the judiciary. Transposition of the international and European law is an important component of the national criminal law and criminal procedure law. There might be however some specificities in legislative provisions depending on the country.

- **European Union level:** The key EU legislative and policy components of this framework are listed below:
  - The EU Directive 2013/40, on Attacks Against Information Systems;
  - The Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013, (Joint Communication To The European Parliament, The

Council, The European Economic And Social Committee And The Committee Of The Regions);

- The EU Directive 2016/1148, Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, “NIS Directive”;
- The EU Regulation 2016/679, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, “General Data Protection Regulation - GDPR”.
- Proposal for Regulation (EU) on European Production and Preservation Orders for Electronic Evidence in Criminal Matters;
- Proposal for a Directive (EU) Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings.
- The European Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (“Blueprint”) (2017);
- The European Commission Communication on Strengthening Europe's Cyber Resilience System (2016);
- The EU Directive 2014/41 Regarding the European Investigation Order in Criminal Matters;
- The EU Regulation 2017/1939 Implementing Enhanced Cooperation on the Establishment of the European Public Prosecutor’s Office (‘the EPPO’);
- The EU Directive 2002/58 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications);
- The EU Directive 2016/680 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data (Law Enforcement Data Protection Directive - LE DP Directive);
- The EU Directive 2016/681 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime (Directive on the Use of Passenger Name Record – PNR - Data);
- The EU Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), (New ENISA Regulation);
- The EU Regulation 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol), (Europol Regulation).

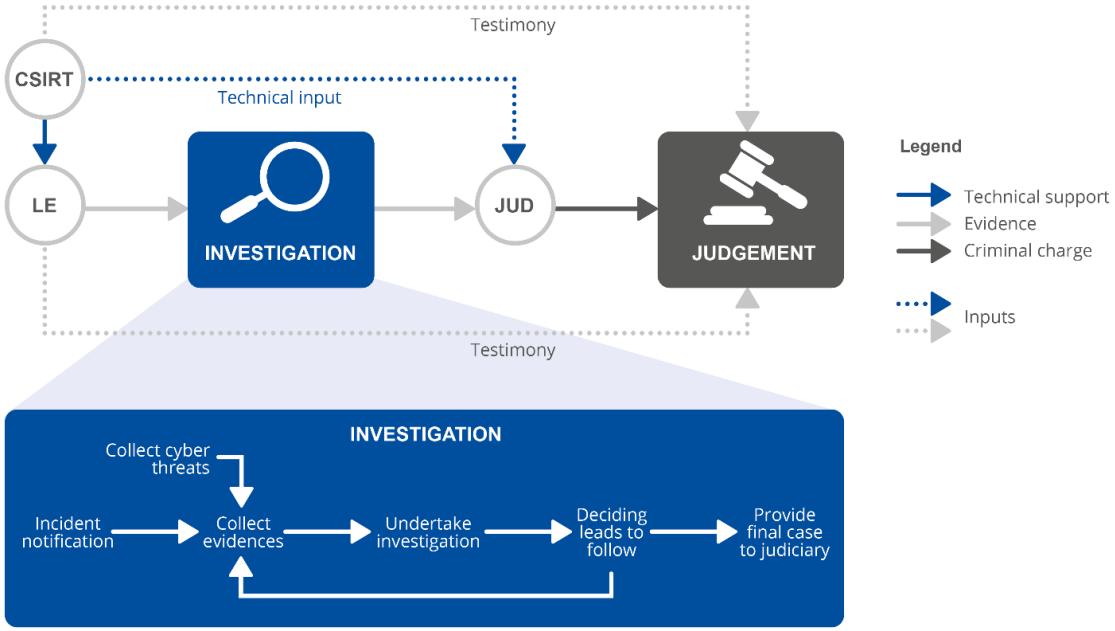
- **International level**:
  - the Council of Europe convention on cybercrime (CETS No.185), "The Budapest Convention"

2.2.2 Information Flow

When suspecting or identifying a security incident or a cybercrime, the competent stakeholders are requested to collect and exchange any type of information that is related to the incident that might be relevant for the investigation. The pieces of information that could be potentially collected and exchanged among CSIRTs, LE and the judiciary include:

- Indicators Of Compromise (IOC)
- IP/email addresses
- Timeline of events
- Decryption keys
- Potential victims/attackers
- Campaign details
- Modi operandi

Figure 2: Graphical representation of the flow of information across CSIRTs, LE and the judiciary



2.2.3 E-evidence admissibility

Electronic evidence has become relevant in a large majority of criminal investigations and increasingly often, judicial authorities need to submit a request to another jurisdiction to obtain necessary evidence from service providers. Making it easier and quicker to obtain this evidence across borders is therefore of crucial importance for investigating and prosecuting crime, including terrorism or cybercrime[1].

[1] European Communication of April 2018 on Fourteenth progress report towards an effective and genuine Security Union (COM(2018) 211)

Additionally, e-evidence collection should be compliant with all the relevant principles, such as data integrity, audit trail, specialist support, appropriate training, chain of custody and legality in order to be considered admissible.

The malleable and volatile nature of electronic evidence (e.g. change of file, memory dumps), challenges their admissibility and hinders the tasks of experts during the collection and preservation stage. If electronic evidence is not properly collected, it might not correspond to the original data and thus compromise the outcome of the criminal investigation (e.g. malware reacts to its investigation and alters the disk/memory).

In order to address and overcome potential drawbacks and difficulties in gathering and handling electronic evidence and avoid gaps in the chain of custody, it is advised to closely examine the set of best practices listed below:

- ISO 27037:2012 - Guidelines for identification, collection, acquisition, and preservation of digital evidence[2]
- NIST Guide to integrating forensic techniques into incident response (SP-800-86)[3]
- ENISA report on Electronic evidence — A basic guide for first responders[4]
- CERT-EU Security white paper on Data acquisition guidelines for investigation purposes[5]
- Guidelines on digital forensic procedures for OLAF staff[6]
- United Kingdom - ACPO Good practice guide for digital evidence[7]

2.2.3.1 E-evidence and GDPR

Depending on the case, **GDPR** (Regulation EU 2016/679) and/or the **Data Protection Law Enforcement Directive** (Directive EU 2016/680) may apply to the CSIRTs when they are collecting, handling, processing and storing personal data.

Under the prism of the GDPR, it should be noted that the processing of personal data by CSIRTs is performed on the legal basis of pursuing the legitimate interests of ensuring network and information security as data controllers or data processors[8]. Provided that the processing of personal data by a CSIRT remains strictly necessary and proportionate for the above mentioned purposes (ensuring network and information security), consent is not the examined legal basis for these processing operations, but instead the processing could be necessary for the purposes of *legitimate interests* pursued by the CSIRTs, and further processing would be

[2] ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence, https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en
[3] SP 800-86 Guide to Integrating Forensic Techniques into Incident Response, https://csrc.nist.gov/publications/detail/sp/800-86/final
[4] ENISA report on Electronic evidence - a basic guide for First Responders, https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders
[5] CERT-EU Security White Paper 2012-004 - Data Acquisition Guidelines for Investigation Purposes External, https://cert.europa.eu/cert/newsletter/en/latest_PublicationsAndNewsletters_.html
[6] Guidelines on Digital Forensic Procedures for OLAF Staff , https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf
[7] ACPO Good Practice Guide for Digital Evidence, http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf
[8] EU Regulation 2016/679 "on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data", Recital 49: "*The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security [...] by computer security incident response teams (CSIRTs) […]"* and Recital 50 *"[…] If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. […] or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. […]"*

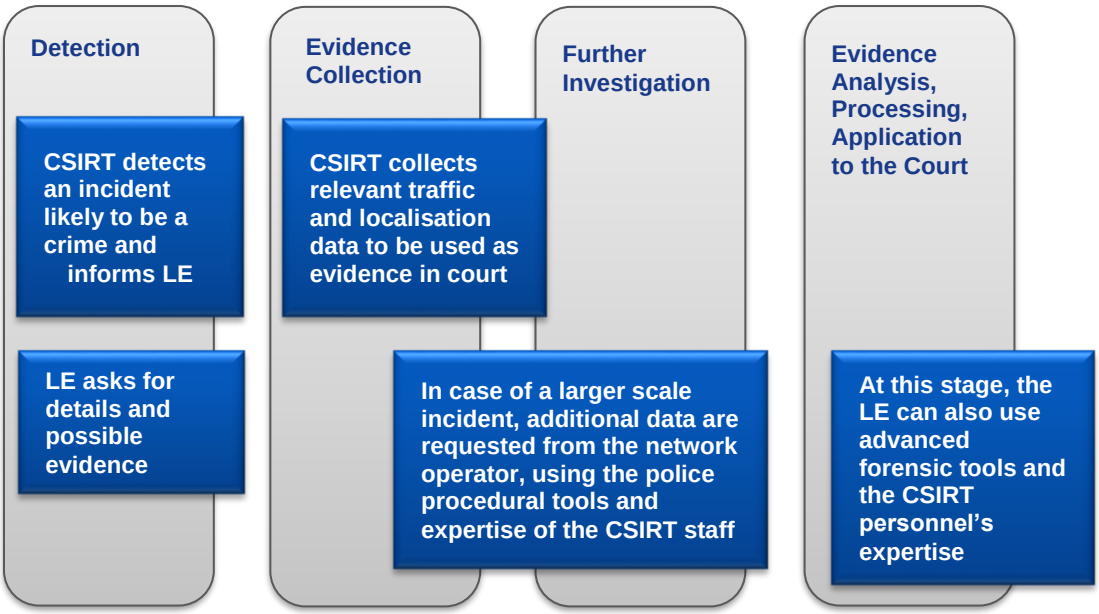
performed *in compliance with their legal obligations* or in the framework of a task carried out *in the public interest* or *in the exercise of official authority* vested in the CSIRTs[9].

When CSIRTs process personal information, (e.g. IP address), on the basis of a specific mandate or delegation from competent authorities (e.g. by a police officer or by the prosecutor) for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the **GDPR does not apply**, but instead the processing is **regulated by the Data Protection Law Enforcement Directive**. However, it should be noted that the provisions of the Directive vary depending on its implementation in each Member State. Additionally, the Directive does not provide specific legal bases for the processing of personal data but instead defines the lawfulness by limiting the processing to activities necessary for performing the tasks carried out by a competent authority for the purposes of *prevention, investigation, detection or prosecution of criminal offences* as further regulated by Member State laws.

2.3 ROLES AND RESPONSIBILITIES

Cooperation among CSIRTs, LE and the judiciary is required through the different stages of an investigation concerning a cybersecurity incident/cybercime, starting from the Detection of an event, to the Evidence Collection process or Further Investigation that may be required and ending at the stage of Evidence Analysis where evidence and expert testimonies are presented at Court. The role of each stakeholder and the workflow of responding to a cybersecurity incident/cybercrime are illustrated in the figure below:

Figure 3: Roles of CSIRTs, LE and the judiciary through the different phases of criminal investigation



A successful and effective cooperation among CSIRTs, LE and the judiciary is built through understanding each stakeholder's role in the state of play and through the implementation of

[9] EU Regulation 2016/679 "on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data", Article 6, par.1 points: (c) *"processing is necessary for compliance with a legal obligation to which the controller is subject;"*, (e) *"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"* and (f) *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party […]."*

appropriate internal procedures to ensure this cooperation. The figure below illustrates both the framework of this cooperation and provide an example of the information flow across the competent authorities.

Figure 4: Cooperation across CSIRT, LE and the judiciary in the course of criminal investigation

Example of cooperation between CSIRT, LE and the Judiciary		
CSIRT	**LE**	**Judiciary**
Internal processes established for **informing the police** and filing complaints with the police and for **collecting evidence** or passing it on to LE.	Implementing means for **secure electronic transfer** of **digital evidence.**	Possibility of using a **CSIRT employee** as an **expert witness**, for explaining to the court the **technical details** of the case and the **specifics of the individual evidence.**
	Adopting procedural measures for cooperation with security teams, including measures for **secure two-way sharing of sensitive information.**	

2.3.1 Role per community

LE and CSIRTs are the first respondents upon the discovery of a cybersecurity incident/cybercrime. A LEA can receive a crime report (e.g. from the victim) or discover a suspicious activity by itself. CSIRTs from their side can discover a suspicious activity during incident handling and depending on the legal system they may have to inform LE/judiciary of the suspicious activity.

Onwards, when the Criminal investigation is launched:

- **LE** conducts the criminal investigation;
- The **Prosecutor** defines the strategy of the case, sets the evidence threshold and supervises it;
- The **judiciary** ensures that the investigation is conducted in compliance with civil liberties and guarantees and defines the limits of protection of the rights of the persons investigated;
- **The CSIRT** may provide technical expertise and supporting the evidence collection (and preservation) by sharing information they have, or they have access to.

2.3.1.1 Role of CSIRTs

CSIRTs deal with incident management and incident handling and thus they have an important role in supporting the investigations by providing information and securing the collection and analysis of e-evidence[10]. CSIRTs do not have the powers of LE vis-à-vis private subjects but as regards attacks of a criminal nature (not all the cyber incidents are criminal acts), have an important role in supporting the investigations, as they can help to provide information and to secure e- evidence.

The main role of the CSIRTs is to protect their constituency by preventing and containing IT security incidents, primarily from a technical point of view. Their duties include:

[10] Council of the European Union, Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime", 2 October 2017

- monitoring incidents at national level;
- providing early warning, alerts, announcements and dissemination of information to relevant stakeholders;
- responding to incidents;
- providing dynamic risk and incident analysis and situational awareness;
- participating in the CSIRT network.

During the incident management and handling process, CSIRTs acquire, store and process data. Therefore, they are required to have an increased awareness regarding the data they process and retain as these can be crucial for the investigation and the prosecution of a crime and during a criminal trial. Bearing in mind the requirements and challenges of e-evidence admissibility, the role of CSIRTs is particularly important at this stage.

2.3.1.2 Role of LE

The role of LE in a cybercrime investigation is concentrated on carrying out the enquiries by collecting and analysing information and evidence on whether a crime has been committed, or is going to be committed, in order to further identify the perpetrator and the affected victims and infrastructures.

LEAs are required to comply with certain legal obligations when collecting evidence, according to the powers conferred on them and under the supervision of the prosecuting authorities. LE may collect evidence directly or may be provided with evidence by other stakeholders.

2.3.1.3 Role of prosecutors and judges

The judiciary acts as a body for the protection of fundamental rights, safeguarding the lawfulness of the investigative procedure. The prosecutors have the authority to order the criminal investigation and are mandated with supervising the investigations duties that are usually conducted by LE.

2.3.2 Segregation of Duties (SoD) matrix

In order to support the three communities to reach a better understanding of each other' duties assigned based on the roles each community has, a SoD matrix (see Figure 5 — Example of segregation of duties matrix) could be drafted at national level. The aim of this matrix is to highlight conflicting or overlapping duties performed by one community or more. As shown in the SoD template below, the CSIRTs, LE, judges and prosecutors have to identify the key responsibilities for their communities and then link them with the skills required in order to fulfil these duties. SoD matrices are usually used to ensure compliance with laws and regulations.

Figure 5: Example of 'Segregation of Duties' matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutor	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training	✓	✓	✓	✓	Problem-solving and critical thinking skills
During the incident/crime					
Evidence collection	✓	✓		✓	Knowledge of what kind of data to collect; organisation skills
Duty to inform other stakeholders/authorities	✓				Obligations and rules for information sharing among communities.
Leading the criminal investigation			✓	✓	Knowledge of the incident response plan; leadership skills
Post incident/crime					
Admitting and assessing the evidence			✓	✓	Evidence in a criminal trial
Reviewing the response and update policies and procedures	✓				Knowledge how to draft an incident response and procedures

2.4 SUMMARY

Through the initial stage of detecting a security incident or a cybercrime and onwards through the criminal investigation, it is observed that CSIRTs interact much more with LE than with the prosecutors and very rarely with the judges. Specific legal provisions regulate the framework of cooperation between CSIRTs, LE and their interaction with the judiciary.

Stakeholders have distinct roles and their strengths and limitations vary depending on their organisational structure. In the framework of this cooperation, CSIRTs have an important role in supporting LE as well as the judiciary through a criminal investigation. Building up a better understanding of the events, suspicious criminal activities that CSIRTs should report to LE and/or the prosecutor as well as of the data that should be collected, can only improve their contribution in this collaboration process. Additionally, there is an increasing need for a more extensive usage of information that can be provided by CSIRTs not only through the stage of criminal investigations but also through the delivery of evidence in court proceedings.

Countering cybercrime requires joint efforts and each community's continuous investment in maintaining a sustainable cooperation through the sharing information. Given the distinct roles of each community and their training needs, an interdisciplinary approach is required to assist these stakeholders in building mutual understanding, overcoming their cultural and institutional limitations and thus mutually benefit from identifying and exploiting the opportunities of cooperation.

3. CASE STUDIES

3.1 CASE STUDY 1

This case study examines the collaboration between CSIRTs and LE when addressing a security incident or a cybercrime as described in a ransomware related scenario. This scenario aims at identifying the roles of each party and thus setting out the means of effective cooperation between them.

Figure 6: Main objective of the case study

Main Objective	
Targeted Audience	CSIRTs and LE
Total Duration	30 minutes
Scenario	Trainee is a CSIRT member responsible for detection and mitigation of security incidents or cybercrimes. His/her goal is to address key ramifications of ransomware attack.
Task 1	List the internal guidelines of identifying security incidents or cybercrimes.
Task 2	List the investigation steps that you could undertake.
Task 3	Identify the type and categories of information that you could collect and share with LE in search of evidence.
Task 4	Identify expected activities of relevant stakeholders by filling in the SoD matrix.
Task 5	List the conclusions that could be derived and the evidence that could be produced.

3.1.1 Objectives

In this exercise, the trainees will learn when and how the CSIRT members cooperate with LE. In particular, the objectives of this exercise are to:

- Practice in identifying cybercrime cases;
- Raise the trainees' awareness regarding the differences between the legal systems of various countries and the consequences of these differences;
- Explain the legal aspects of CSIRT activity;
- Practice in writing instructions regarding the reporting of a cybercrime to LE;
- Provide information on how to advise LE in the event of a security incidents or cybercrimes.

3.1.2 Scenario

A ransomware attack has been launched through the following steps:

- **The attacker gathered information online and collected email addresses of several organisations.**
- **The attacker sent a malicious word file through an email to all these addresses.**
- **Some users opened the word file.**
- **The malicious payload of the word file downloaded a binary that was executed.**
- **The payload encrypted the files of the current user.**
- **The attacker requests ransom to be paid to a crypto wallet**

3.1.2.1 Organisational profile

Your organisation is a national CSIRT team responsible for detection and mitigation of cybersecurity incidents/cybercrimes.

3.1.2.2 Before the breach

The CSIRT provided its constituency with guidelines on how to identify and report incidents.

A LEA submits an official letter to a CSIRT in order to obtain the required information and investigate an individual incident:

- List the type and categories of data that should be included in that official letter.
- Provide advice on the data requested for each individual incident and list the obligatory and the optional information that should be requested.

Please note that specific rules, policies and guidelines apply in each national LE or CSIRT constituency. For example, identify the following:

- How long is data concerning IP addresses assignments stored?
- What data should the CSIRTs provide to the LE?

3.1.2.3 Initial response

Examples of questions that could be addressed by LE during the investigation process:

- LE asks for the list of log entries that could help to identify users connecting to the internet using computer with IP address ‘xxxx’.
- LE asks to identify the user to whom the IP address ‘xxxxx’ was assigned in a specific period of time, e.g. a few years ago (WHOIS issues)

3.1.2.4 Investigation analysis

List the type and categories of information that could be potentially shared with LE during the investigation process of the above described scenario:

- Email message
- IPs of infected hosts
- User log files
- Hash of the Word file or the word file itself
- Payload
- Downloaded binary or its hash
- IP used to collect the binary
- Wallet address

- Screenshots of the ransomware message
- Address of the message containing the ransomware message
- Memory dumps
- Network logs (infected client/mail server)
- Samples of encrypted files
- Images of the hard drives

3.1.2.5 Segregation of Duties

Use the SoD matrix (Figure 7) to identify, what activities can be performed or facilitated by your CSIRT, and what you expect from the LE. The SoD matrix should help you also to identify, what kinds of information and data could be useful for the LE and what kinds of data you can request from them and use for mitigating the attack.

3.1.2.6 Outcomes

Through the investigation analysis and the correlation of data shared with LE we could derive the following conclusions and collect the evidence listed below:

- Traffic of the crypto wallet
- Details about the IP that delivered the binary
- Details about other activity of the downloaded binary
- Usage in other campaigns
- Possible keys (extracted from the memory dump/network traffic/used in other campaigns)
- Decryptor for the binary
- Correlation with other similar events
- Indicators of Compromise for other cases
- Origin of the email (internal/external)
- Email/IP addresses used to send the email
- Email metadata

3.1.3 Lessons learned

Having set internal policies and guidelines on the information that could be collected and shared through the CSIRT with LE, assisted the communities in drawing conclusions and producing valuable evidence for investigating and responding to this cybersecurity incident.

Figure 7: 'Segregation of Duties' matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training	✓	✓	✓	✓	Problem-solving and critical thinking skills
Collecting cyber threat intelligence	✓	✓		✓	Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats	✓	✓		✓	Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats	✓				Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime	✓	✓			Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime	✓	✓			Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime	✓	✓		✓	Incident and crime classification and identification
Identify the type and severity of the compromise	✓	✓		✓	Knowledge of cyber threats and incident response procedures
Evidence collection	✓	✓		✓	Knowledge of what kind of data to collect; organisation skills
Providing technical expertise	✓				Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial	✓	✓		✓	Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)	✓			✓	Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime	✓	✓		✓	Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)	✓				Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling	✓				Communication skills; communication channels
Mitigation of an incident	✓				Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation		✓		✓	Knowledge of the legal framework; decision-making skills
Leading the criminal investigation			✓	✓	Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation			✓	✓	Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE		✓	✓	✓	Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution	✓	✓	✓	✓	Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery	✓				Technical skills
Protecting the constituency	✓				Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view	✓				Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence		✓	✓	✓	Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE			✓	✓	Testimonies in a criminal trial
Admitting and assessing the evidence			✓	✓	Evidence in a criminal trial
Judging who committed a crime			✓		Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost	✓	✓	✓	✓	Evaluation skills
Reviewing the response and update policies and procedures	✓				Knowledge how to draft an incident response and procedures

**Differences may be highlighted in this matrix depending on the legal framework of each Member State.*

This is just an indicative example.

3.2 CASE STUDY 2

This case study examines the collaboration between CSIRTs and LE when addressing a cybersecurity incident as described in a Denial of Services (DoS) attack scenario. Through this scenario we aim at identifying the roles of each party and thus setting out the means of effective cooperation between them.

Figure 8: Main objective of the case study

Main Objective	
Targeted Audience	CSIRTs and LE
Total Duration	30 minutes
Scenario	Trainee is a CSIRT member responsible for detection and mitigation of security incidents or cybercrimes . His/her goal is to address key ramifications of DoS attack.
Task 1	List the internal guidelines of identifying security incidents or cybercrimes.
Task 2	List the investigation steps that you could undertake.
Task 3	Identify the type and categories of information that you could collect and share with LE.
Task 4	Identify expected activities of relevant stakeholders by filling in the SoD matrix.
Task 5	List the conclusions that could be derived and the evidence that could be produced.

3.2.1. Objectives

In this exercise, the trainees will learn when and how CSIRT members cooperate with LE. In particular, the objectives of the exercise are to:

- Practice in identifying cybercrime cases;
- Raise the trainees' awareness regarding the differences between the legal systems of various countries and the consequences of these differences;
- Explain the legal aspects of CSIRT activity;
- Practice in writing instructions regarding the reporting of a cybercrime to LE;
- Provide information on how to advise a reporter or LE in the event of a security incident or a cybercrime.

3.2.2. Scenario

The DoS was launched through the following steps:

- **The attacker gathered information online and identified some web servers**
- **The attacker submitted some content to the web servers**
- **The web servers went "down" and do not provide their service**

3.2.1.1 Organisational profile

Your organisation is a national CSIRT responsible for the detection and mitigation of cybersecurity incidents/cybercrimes.

3.2.1.2 Before the breach

The CSIRT provided its constituency with guidelines on how to identify and report incidents.

A LEA submits an official letter to a CSIRT in order to obtain the required information and investigate an individual incident:

- List the type and categories of data that should be included in that official letter.
- Provide advice on the data requested for each individual incident and list the obligatory and the optional information that should be requested.

Please note that specific rules, policies and guidelines apply to each national LE or CSIRT constituency. For example, identify the following:

- How long is data concerning IP addresses assignments stored?
- What data should the CSIRTs provide to the LE?

3.2.1.3 Investigation analysis

List the type and categories of information that could be potentially shared with LE during the investigation process of the above described scenario:

- IPs of servers
- User log files of the servers
- Payload of that led to the DoS
- IP used to send the payload
- Memory dumps
- Network logs (web server/other devices)
- Images of the hard drives

3.2.1.4 Segregation of Duties

Use the SoD matrix (Figure 9) to identify, what activities can be performed or facilitated by your CSIRT, and what you expect from the LE. The SoD matrix should help you also to identify, what kinds of information and data could be useful for the LE and what kinds of data you can request from them and use for mitigating the attack.

3.2.1.5 Outcomes

Through the investigation analysis and the correlation of data shared with LE we could derive the following conclusions and collect the evidence listed below:

- Details about the IP that delivered the payload
- Details about other activity in the web server
- Usage in other campaigns
- Zero-day exploit
- Correlation with other similar events
- Indicators of Compromise for other cases

3.2.3. Lessons learned

Having set internal policies and guidelines on the information that could be collected and shared through the CSIRT with LE, assisted the communities in drawing conclusions and producing valuable evidence for investigating and responding to this cybersecurity incident.

Figure 9: 'Segregation of Duties' matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training	✓	✓	✓	✓	Problem-solving and critical thinking skills
Collecting cyber threat intelligence	✓	✓		✓	Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats	✓	✓		✓	Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats	✓				Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime	✓	✓			Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime	✓	✓			Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime	✓	✓		✓	Incident and crime classification and identification
Identify the type and severity of the compromise	✓	✓		✓	Knowledge of cyber threats and incident response procedures
Evidence collection	✓	✓		✓	Knowledge of what kind of data to collect; organisation skills
Providing technical expertise	✓				Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial	✓	✓		✓	Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)	✓			✓	Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime	✓	✓		✓	Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)	✓				Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling	✓				Communication skills; communication channels
Mitigation of an incident	✓				Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation		✓		✓	Knowledge of the legal framework; decision-making skills
Leading the criminal investigation			✓	✓	Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation			✓	✓	Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE		✓	✓	✓	Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution	✓	✓	✓	✓	Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery	✓				Technical skills
Protecting the constituency	✓				Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view	✓				Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence		✓	✓	✓	Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE			✓	✓	Testimonies in a criminal trial
Admitting and assessing the evidence			✓	✓	Evidence in a criminal trial
Judging who committed a crime			✓		Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost	✓	✓	✓	✓	Evaluation skills
Reviewing the response and update policies and procedures	✓				Knowledge how to draft an incident response and procedures

**Differences may be highlighted in this matrix depending on the legal framework of each Member State.*

This is just an indicative example.

4. REFERENCES

ENISA. (2017). *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement.* Retrieved from https://www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement

ENISA. (2017a). *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects.* Retrieved from https://www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement

ENISA. (2018). *Cooperation between CSIRTs and law enforcement: interaction with the judiciary.* Retrieved from https://www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement

ENISA. (2018a). *Review of Behavioural Sciences Research in the Field of Cybersecurity.* Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/

A ANNEX: ABBREVIATIONS

Abbreviation	Description
CSIRT	Computer Security Incident Response Team
DoS	Denial-of-Service (attack)
GDPR	General Data Protection Regulation
IOC	Indicators Of Compromise
IP	Internet Protocol
LE	Law Enforcement
LEA	Law Enforcement Agency
SoD	Segregation (or separation) of Duties

TP-01-20-173-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-332-2
DOI: 10.2824/27536